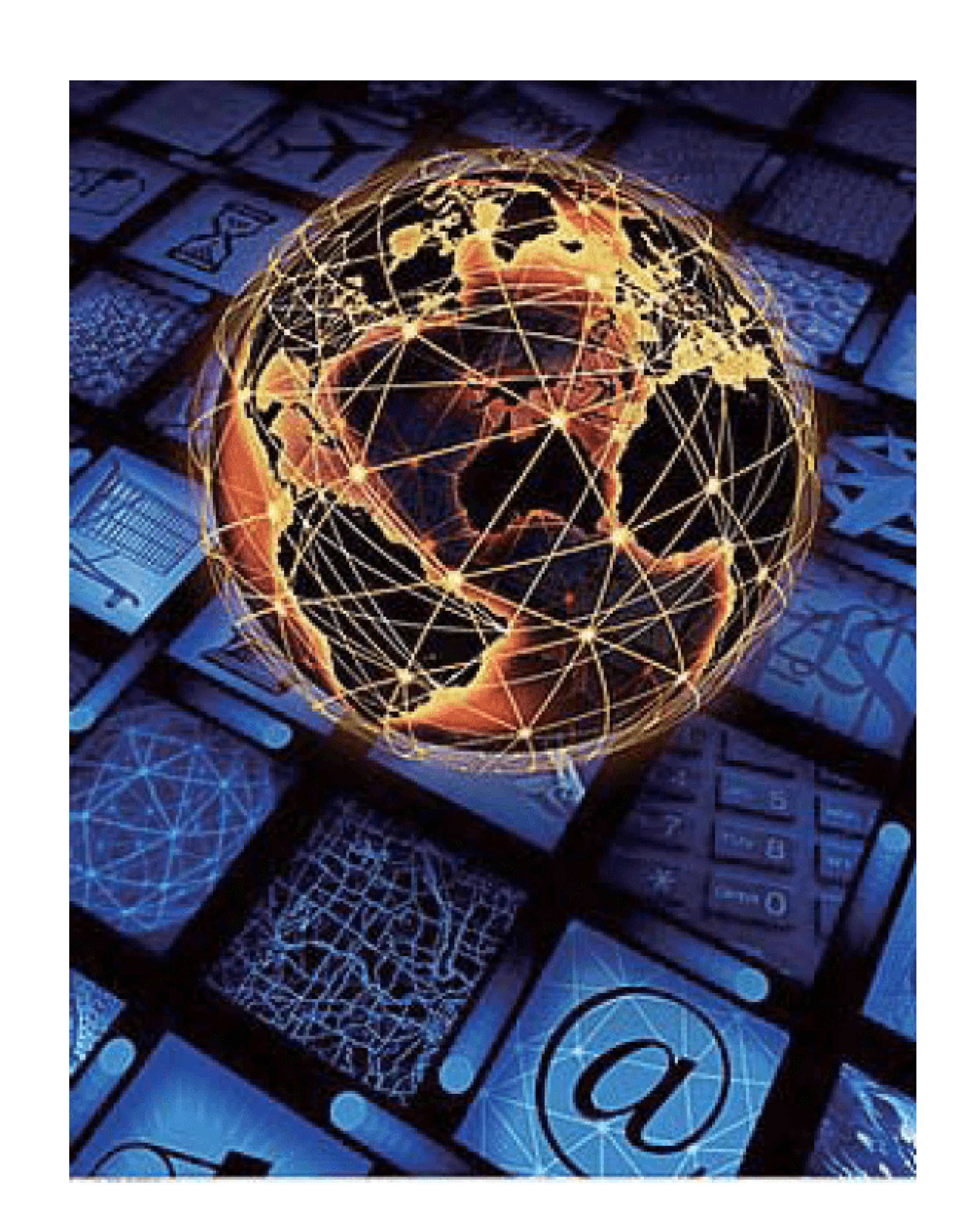
高等学校计算机应用规划教材

Windows Server 2008 系统管理

- Windows Server 2008初步使用
- 文件服务
- 信息共享服务
- DNS服务
- 活动目录服务
- 证书服务
- DHCP服务
- Web服务
- FTP服务
- 邮件服务
- 流媒体服务
- 终端服务
- 代理服务
- 系统安全防护
- 综合应用案例



姚青山　主 编

谷春英 金振乾 谢伟增　副主编

清华大学出版社

高等学校计算机应用规划教材

Windows Server 2008 系统管理

姚青山　主　编

谷春英　金振乾　谢伟增　副主编

清华大学出版社

北　京

内 容 简 介

本书全面介绍了功能强大、稳定性强、安全性高的微软公司新一代网络服务器操作系统 Windows Server 2008。全书共分为 15 章，分别介绍了 Windows Server 2008 的安装和初步使用以及文件服务、信息共享服务(WSS)、DNS 服务、活动目录服务、证书服务、DHCP 服务、Web 服务、FTP 服务、邮件服务、流媒体服务、终端服务、代理服务的配置与管理以及系统安全防护的配置和管理，并通过一个综合案例介绍了以上各种技术的应用。

本书内容丰富，体系完整；阐述详尽，强化应用；图文并茂，易学易用；资源配套，便于教学。各部分内容相辅相成，文字简洁清晰，丰富的插图配合文字说明，将 Windows Server 2008 系统的配置和管理叙述清晰、完整。配有大量思考题和练习题，便于巩固所学。本书主要面向服务器系统构建和管理的学习者，适合作为信息类专业应用型本科学生的网络操作系统应用教程，也可作为该课程培训班的培训教材、高职高专教学的参考书，对于服务器系统管理人员也具有较高的参考价值。

本书的电子教案和习题答案可以到 http://www.tupwk.com.cn/downpage 网站下载。

图书在版编目(CIP)数据

Windows Server 2008 系统管理 / 姚青山　主编. —北京：清华大学出版社，2013.2

(高等学校计算机应用规划教材)

ISBN 978-7-302-31251-2

Ⅰ. ①W…　Ⅱ. ①姚…　Ⅲ. ①Windows 操作系统—网络服务器—系统管理—高等学校—教材　Ⅳ. ①TP316.86

中国版本图书馆 CIP 数据核字(2013)第 002296 号

责任编辑：胡辰浩　袁建华
装帧设计：康　博
责任校对：蔡　娟
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62794504
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**25.75　　**字　　数：**595 千字
版　　次：2013 年 2 月第 1 版　　**印　　次：**2013 年 2 月第 1 次印刷
印　　数：1～5000
定　　价：46.00 元

产品编号：

前　　言

微软公司推出的 Windows 操作系统产品以其易用性和庞大的第三方软件支撑体系，占据了绝对的市场份额，拥有庞大的用户群。新的网络服务器操作系统 Windows Server 2008 继承了 Windows 系列产品的优势，并大大扩充了其功能，强化了包括稳定性和安全性在内的系统性能，受到了服务器系统管理人员的欢迎。

全书共分为 15 章，按照内容之间的关系依次介绍了 Windows Server 2008 操作系统的各个主要功能，利用这些功能，可以架设起多种功能的服务器系统，提供完备的网络服务。

各章的主要内容如下：

第 1 章介绍了 Windows Server 2008 的安装和初步使用。主要包括 Windows Server 2008 的概述、安装、初步使用、基本的配置和管理、启动故障排除。

第 2 章介绍了 Windows Server 2008 的文件服务配置和管理。主要包括 Windows Server 2008 的文件服务与资源共享、NTFS 权限、磁盘配额与分布式文件系统。

第 3 章介绍了 Windows Server 2008 的信息共享服务(WSS)配置和管理。主要包括安装 WSS 服务、管理 WSS 站点与使用 WSS 模板。

第 4 章介绍了 Windows Server 2008 的 DNS 服务配置和管理。主要包括 DNS 服务概述、安装、配置与管理、安装辅助 DNS 服务器。

第 5 章介绍了 Windows Server 2008 的活动目录服务配置和管理。主要包括活动目录概述、活动目录的安装、配置与删除、用户与组的管理、Windows 计算机加入域、登录域、脱离域、组策略及应用。

第 6 章介绍了 Windows Server 2008 的证书服务配置和管理。主要包括电子证书服务、企业 CA 的安装与使用。

第 7 章介绍了 Windows Server 2008 的 DHCP 服务配置和管理。主要包括 DHCP 服务概述、安装 DHCP 服务器、DHCP 服务器的设置、DHCP 服务器的维护与 DHCP 客户端的配置。

第 8 章介绍了 Windows Server 2008 的 Web 服务配置和管理。主要包括 Web 服务的搭建与配置、Web 服务器的管理、搭建 SSL Web 网站。

第 9 章介绍了 Windows Server 2008 的 FTP 服务配置和管理。主要包括 FTP 服务器的搭建与配置、为 FTP 设置 NTFS 访问权限、虚拟站点与虚拟目录、FTP 站点的访问安全和 FTP 站点的访问。

第 10 章介绍了 Windows Server 2008 的邮件服务配置和管理。主要包括 Exchange Server 2007 概述、安装 Exchange Server 2007、使用 Exchange 管理控制台建立用户邮箱、客户端的使用、配置面向 Internet 的集线器传输服务器、邮箱常用操作和限制。

第 11 章介绍了 Windows Server 2008 的流媒体服务配置和管理。主要包括流媒体服务的安装、实现点播和广播。

第 12 章介绍了 Windows Server 2008 的终端服务器配置与管理。主要包括部署终端服务器、部署终端服务的客户端、部署终端服务应用程序、配置客户端的应用环境和在客户端计算机访问 TS 服务器上的应用程序。

第 13 章介绍了 Windows Server 2008 的代理服务器配置与管理。主要包括 Forefront TMG 概述、安装与配置、客户端代理上网的设置。

第 14 章介绍了 Windows Server 2008 的安全防护配置与管理。主要包括系统更新配置、防火墙配置、防病毒配置、防间谍配置。

第 15 章是将以上各种 Windows Server 2008 技术进行综合应用的一个案例。主要包括网络结构设计与连接以及主机系统配置。

本书的特色主要有：

(1) 内容丰富，阐述详尽，强化应用。本书作者来自网络操作系统教学和应用的第一线，对包括 Windows Server 2008 在内的网络操作系统的配置与管理有深入的理解和较为丰富的应用经验，这些理解和经验贯穿于本书始终；在介绍 Windows Server 2008 相关技术时做到了围绕应用、详尽阐述。

(2) 图文并茂，易学易用。为了增强可理解性和易学易用性，各章节介绍 Windows Server 2008 相关技术时文字简洁清晰，丰富的插图配合文字说明，章始有导读，章末有小结，将配置和管理细节叙述得清晰、完整。

(3) 资源配套，便于教学。各章最后配有针对性的思考和练习题，帮助读者加深理解、学以致用；各章均送教学课件，便于教师教学。

本书主要面向服务器系统构建和管理的学习者，适合作为信息类专业应用型本科学生的网络操作系统应用教程，也可作为该课程培训班的培训教材、高等院校教学的参考书，对于服务器系统管理人员也具有较高的参考价值。

本书由姚青山担任主编，确定本书的编写风格、写作思路和内容结构，完成组稿和统稿工作，并参与了部分章节的编写工作。金振乾编写了第 1 章、第 4 章和第 9 章；谢伟增编写了第 2 章和第 3 章；姚青山编写了第 5 章、第 13 章、第 14 章和第 15 章；高继勋编写了第 7 章和第 12 章；谷春英编写了第 6 章、第 8 章和第 11 章；宋三柱编写了第 10 章。在编写过程中，清华大学出版社给予了大力支持和有力帮助，同时，卫琳、陶永才、张宁宁、任国明、贾伟伟、朱居正、张龙涛、景京、周梦雪、代琳娜、王冬、谢涛、王晓慧、何宗真、李文洁、王强、白娟等参与了部分工作，参编人员参考了诸多同仁出版或发表的大量文献和资料，在此一并表示感谢。

尽管编者在多个方面都做了大量工作，但由于经验有限和时间仓促，加之相关技术发展日新月异，书中难免有不尽人意之处，还恳请广大读者不吝赐教，对本书的宝贵意见和建议可发送到邮箱 huchenhao@263.net，也可拨打电话 010-62796045。

编　者

2012 年 8 月

目　　录

第1章　Windows Server 2008 初步使用

【本章导读】

Windows Server 系列操作系统是微软公司开发的网络操作系统，界面直观，易学易用，是中小型网络服务器的首选操作系统。其中最新的 Windows Server 2008 更是在前作的基础上做了大刀阔斧的修改，无论是功能还是性能均获得了极大的提升，在安装方式、使用方法方面有了较大改进，在安全特性上有明显的提高。本章着重介绍了 Windows Server 2008 的新特性、安装方法、配置操作和常用操作。通过本章的学习，读者可以根据实际需要选择适合自己的版本，恰当的安装方式，并能进行简单的操作和配置，为进一步设置 Windows Server 2008 服务器的功能、提高服务器的安全性、处理运行中出现的异常情况打下基础。

1.1　系统概述

1.1.1　系统简介

Windows Server 2008 是微软公司目前所开发出的最新、最安全、性能最好的网络操作系统。微软公司在已经大获成功的 Windows Server 2003 系列网络操作系统的基础上，保留特色功能，取消用户不甚满意的部分，增加了虚拟化等新功能，并强调安全性和易用性，开发出了 Windows Server 2008 系列操作系统。

Windows Server 2008 可以帮助用户最大限度地控制其基础结构，同时提供空前的可用性和管理功能，使用户可以建立比以往更加安全、可靠和稳定的服务器环境。Windows Server 2008 可确保处于任何地理位置的用户都能从网络获取完整的服务，从而为组织带来新的价值。Windows Server 2008 还具有对操作系统深入洞察和诊断的功能，使管理员能够将更多的时间用于创造业务价值。

Windows Server 2008 虽然是建立在优秀的 Windows Server 2003 操作系统的成功和实力，以及 Service Pack 1 和 Windows Server 2003 R2 中采用的创新技术的基础之上的，但是，Windows Server 2008 不仅仅是先前各操作系统的提炼，Windows Server 2008 旨在为组织提供最具生产力的平台，它为基础操作系统提供了令人兴奋的许多重要新功能，并

促进应用程序、网络和 Web 服务从工作组转向数据中心。

除了新功能之外，与 Windows Server 2003 相比，Windows Server 2008 还对基础操作系统进行了功能改进。重要功能改进包括：对网络、高级安全功能、远程应用程序访问、集中式服务器角色管理、性能和可靠性监视工具，故障转移群集、部署以及文件系统的改进。上述功能改进和其他改进可帮助组织最大限度地提高灵活性、可用性和对其服务器的控制。

1.1.2　系统的新特性

Windows Server 2008 相比 Windows 以往版本的操作系统，增加了很多新特性和新功能。其中主要的新功能有以下 5 点。

1. Server Core 模式

这是相比以前 Windows 各版本操作系统最大的变化。Windows 系列操作系统一直以图形用户界面作为自己的主要特色。然而在网络操作系统中，图形用户界面却不是必须的，甚至是会产生负面影响的。如果操作系统采用图形用户界面，那么必须有许多相关程序对其进行支持，如显卡驱动程序，鼠标动作的监视和响应程序等，在提高易用性的同时，增加了系统的复杂性和提高了对计算机硬件的需求，降低了系统响应速度，同时也会增加系统出现 BUG 和被攻击的可能性。Server Core 模式取消了图形用户界面，采用命令行对系统进行配置，取消了和网络服务无关的程序和功能模块，提高了系统的运行速度和安全性。对于普通用户来说，计算机操作系统的易用性是第一位的，硬件性能及其利用率并不那么重要，因此图形用户界面对普通用户来说是非常重要的；对于网络管理员来说，网络操作系统应该可以充分发挥硬件的性能，提高使用率，同时具有较高的安全性和可靠性，而且网络管理员往往具有较高的计算机应用水平，因此取消图形用户界面、采用 Server Core 模式对于服务器来说是一个很好的选择。

2. PowerShell 命令行

PowerShell 原来是 Windows Vista 的一部分，但当时只是作为免费下载的增强附件，随后又成了 Exchange Server 2007 的关键组件，接下来又是 Windows Server 2008 不可或缺的一个成员。这个新的命令行工具可以作为图形界面管理的补充，甚至可以彻底取代图形管理界面。

3. 虚拟化技术

微软的虚拟化技术称为 Hyper-V。简单来说，操作系统方面的虚拟化技术就是一种在一个计算机硬件平台上同时运行多个操作系统的技术。该技术可以在不过分降低性能的同时充分利用计算机的硬件资源，提高运行效率，提高可靠性，同时不增加或者降低成本。微软公司的虚拟化技术是同时支持 Intel 和 AMD 两大 CPU 厂商的虚拟化技术，因此即使在不同的平台上使用 Windows Server 2008，也都可以获得上佳表现。

4. 自修复 NTFS 文件系统

该功能可以随时发现采用 NTFS 文件系统的硬盘空间的问题并加以修复，而且不需要像以前的操作系统那样必须重新启动才可以完成查错和修复，减少了重启次数，提高了工作效率。

5. 增强的安全性

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业发布 Windows Server 2008 正式版的运营和发展奠定了坚实的基础。Windows Server 2008 提供了减小内核攻击面的安全创新，因而使服务器环境更安全、更稳定。通过保护关键服务器服务使之免受文件系统、注册表或网络中异常活动的影响，Windows 服务强化有助于提高系统的安全性。借助网络访问保护(NAP)、只读域控制器(RODC)、公钥基础结构(PKI)增强功能、Windows 服务强化、新的双向 Windows 防火墙和新一代加密支持，Windows Server 2008 操作系统中的安全性也得到了增强。

1.1.3　系统版本

Windows Server 2008 有标准版、企业版和数据中心版三大系列，每一系列均根据所支持的中央处理器技术的不同，又分为支持 32 位 CPU 和支持 64 位 CPU 的版本，可以满足不同用户和硬件平台的需求，无论是小型企业用户，还是全球性的大型分布式网络环境，均可以找到适合的版本。针对 Intel 公司的安腾(Itanium)系列 CPU，还有专用的 Windows Server 2008 安腾版可供选择。此外还有 3 个不支持虚拟化技术的版本。

1. Windows Server 2008 标准版

Windows Server 2008 标准版是一个性能优异、可靠性高的网络操作系统，可以快捷、方便地提供企业解决方案，拥有强大的网络部署和管控功能，能够为用户节约大量的人力和财力。Windows Server 2008 标准版主要为小型企业和部门应用而设计，具备了大多数网络需要的基本功能，并具有全能的 Server Core 安装选项，通常用于文件和打印机共享、Internet 安全连接等，允许集中化的桌面应用程序部署。

Windows Server 2008 32 位标准版最大可支持 4G 内存和最多 4 个 CPU 核心，而 64 位标准版最大可支持 32G 内存。

2. Windows Server 2008 企业版

Windows Server 2008 企业版是为了满足各种规模的企业的一般用途而设计，是一种全功能的网络操作系统，能够提供高度可靠性和强大的性能，是构建各种应用程序、Web 服务器和基础结构的理想平台。企业版在功能类型上与标准版基本相同，但通过支持更高级的硬件系统，可以提供更强大的性能，同时可以提供更加优秀的可伸缩性和可用性，增加了一些企业及应用的支持，如 Failover Clustering 与活动目录联合服务等。Windows Server

2008 企业版适用于更大规模的网络，支持更多数量的用户和更复杂的网络应用。

Windows Server 2008 32 位企业版最大可支持 64G 内存和最多 8 个 CPU 核心，而 64 位企业版最高可以支持 2T 内存。

3. Windows Server 2008 数据中心版

Windows Server 2008 数据中心版是为运行企业和任务所倚重的应用程序而设计的，这些应用程序需要最高的可伸缩性和可用性，是微软公司所有操作系统中功能最强大的。Windows Server 2008 32 位数据中心版支持最大 64G 内存和最多 32 个 CPU 核心，提供 8 节点群集和负载平衡服务，64 位数据中心版最高可支持 2T 内存。

4. Windows Server 2008 安腾版

Windows Server 2008 安腾版是专为 Intel 安腾系列 64 位 CPU 而设计，可以充分发挥安腾处理器的强大性能，并且支持最高 2T 内存，但由于硬件平台的差异，Windows Server 2008 安腾版不具备其他版本的部分功能。

1.2　系统的安装

Windows Server 2008 是微软公司目前最先进的操作系统，比以往的操作系统在安全性、稳定性及功能等方面都有相当大的提高，其安装方式也借鉴了 Windows Vista 和 Windows 7，大大简化了安装流程，缩短了安装时间。

1.2.1　安装要求

Windows Server 2008 对计算机硬件配置要求较高，而且不同版本的系统对计算机硬件配置要求也有所不同，各版本的硬件设备要求如表 1-1 所示。

表 1-1　Windows Server 2008 硬件需求

需　求	标准版	企业版	数据中心版	安腾版
CPU 最低频率	32 位：1GHz 64 位：1.4GHz	32 位：1GHz 64 位：1.4GHz	32 位：1GHz 64 位：1.4GHz	Itanium 2 系列处理器
CPU 推荐频率	2GHz 或更高	2GHz 或更高	2GHz 或更高	2GHz 或更高
内存最小容量	512MB	512MB	1GB	1GB
内存推荐容量	2GB	3GB	2GB	2GB
内存最大容量	32 位：4GB 64 位：32GB	32 位：64GB 64 位：2TB	32 位：64GB 64 位：2TB	2TB
多 CPU 支持	1~4	1~8	8~32	1~64

(续表)

需　求	标准版	企业版	数据中心版	安腾版
所需磁盘空间	最小 10GB 推荐 40GB 及以上	最小 10GB 推荐 40GB 及以上	最小 10GB 推荐 40GB 及以上	最小 10GB 推荐 40GB 及以上
群集节点数	无	最多 8 个	最多 8 个	

Windows Server 2008 中的 64 位版本对硬件兼容性要求较高，安装 64 位系统的计算机硬件必须安装通过微软认证的、具有数字签名的核心模式驱动程序，否则会被拒绝安装。虽然也可以在计算机启动时按下 F8 键，选择高级启动模式，从而禁用驱动程序的签名检查，但是不推荐采用这种方法将 Windows Server 2008 安装到具有不兼容的硬件的计算机上，这样会导致计算机运行不稳定或不能充分发挥 Windows Server 2008 系统的性能。

此外，Windows Server 2008 系统安装光盘为 DVD 光盘，因此安装 Windows Server 2008 的计算机上必须具有 DVD 光驱。

安装前还需要注意以下事项：

- 确保计算机硬件兼容 Windows Server 2008 操作系统，并满足最低需求。
- 确保计算机和外界网络实现物理隔离。
- 不必要的设备应在安装系统前断开与计算机的连接，如扫描仪、打印机等。
- 将操作系统安装至全新分区，并使用 NTFS 文件系统，不要使用第三方分区工具。
- 为硬盘分区时，为系统安装文件、数据文件和日志文件划分不同的分区。
- 不要在服务器上安装多个操作系统。
- 如果采用升级安装而非全新安装，备份原系统的重要文件，并确保原系统无重大故障。

1.2.2　安装方式

根据不同的用户需求，Windows Server 2008 系统提供了不同的安装方式。Windows Server 2008 为用户提供了以下几种安装方式。

1. 全新安装

全新安装是最基本的安装方式，安装时使用 Windows Server 2008 系统光盘启动计算机，然后根据安装提示进行适当操作，即可完成安装。全新安装是最安全的安装方式，推荐用户使用全新的服务器或完全更换系统时采取此种方式。

2. 升级安装

如果计算机中原来安装有 Windows Server 2003 操作系统，并且已经运行了一些必要的、不可间断的服务，则可考虑升级安装的方式。升级安装可以将 Windows Server 2003 系统升级至 Windows Server 2008，同时不改变原有的服务和设置。

Windows Server 2003 标准版(安装 SP1 级以上版本的补丁包)可升级至 Windows Server 2008 标准版和企业版，Windows Server 2003 企业版(安装 SP1 级以上版本的补丁包)只能升级至 Windows Server 2008 企业版。

3. 通过 Windows 部署服务远程安装

Windows Server 2008 还可以通过网络从 Windows 部署服务器安装，并可以通过应答文件实现自动安装。要实现远程安装，计算机必须支持 PXE 功能。

4. Server Core 安装

除 Windows Server 2008 安腾版外，其他版本均支持 Server Core 安装。使用该模式安装的 Windows Server 2008 不具备图形用户界面，管理员通过命令行管理服务器，而且只集成了部分应用和功能，因此更加安全和可靠，同时降低了管理的难度。推荐水平较高的管理员在追求高性能和高稳定性时采取这种安装方法。

1.2.3　全新安装

全新安装是最安全、最高效的安装方式，也是微软公司推荐的安装方式。操作步骤如下：

(1) 使用 Windows Server 2008 安装光盘启动计算机，进入 Windows Server 2008 安装向导界面，如图 1-1 所示。如果要安装简体中文版的系统，使用如图 1-1 所示的配置即可，如果要安装其他语言，则根据需要选择适当选项。



图 1-1　安装向导界面

(2) 单击“下一步”按钮，提示即将开始安装，如图 1-2 所示，在该界面，用户可以单击“安装 Windows 须知”了解安装系统时应注意的问题，或直接单击“现在安装”以进行安装。



图 1-2　安装选项界面

(3) 单击“现在安装”后，系统进入“选择要安装的操作系统”界面，如图 1-3 所示。此界面中罗列了目前可以安装的操作系统版本。本书以 Windows Server 2008 企业版为例，因此选择“Windows Server 2008 Enterprise(完全安装)”。如果用户要使用 Server Core 模式进行安装，则可选择带有“服务器核心安装”字样的对应选项。

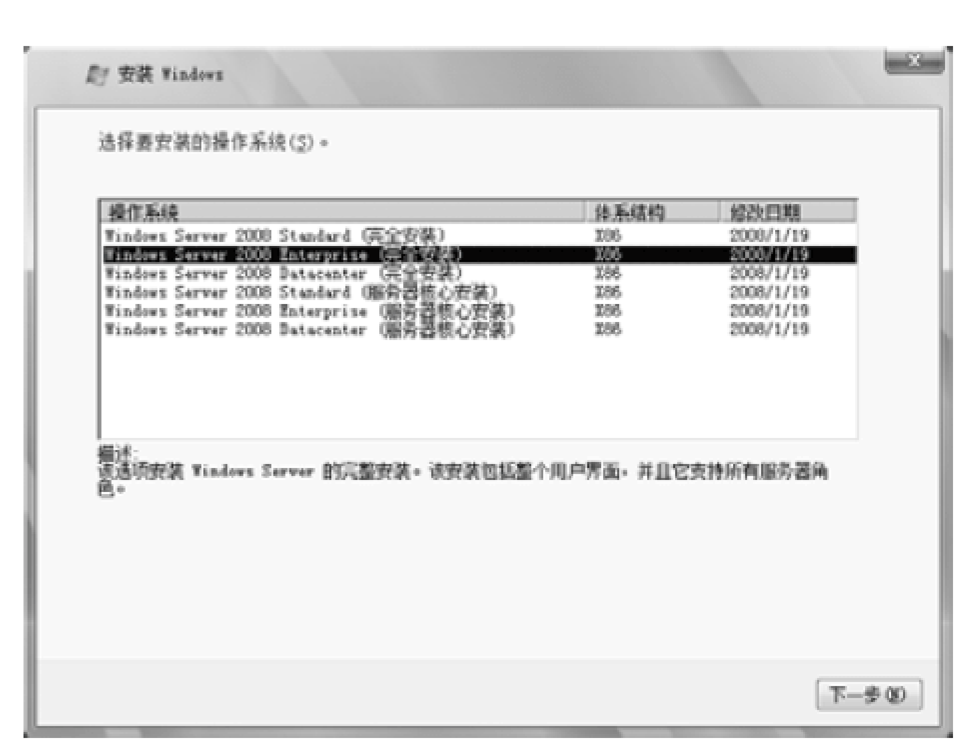


图 1-3　安装版本选择界面

(4) 选择好安装的版本后，单击“下一步”按钮，进入“请阅读许可条款”界面，如图 1-4 所示。本界面显示了系统用户的权利和义务。



图 1-4　安装协议界面

(5) 选中“我接受许可条款”复选框，单击“下一步”按钮，进入“您想进行何种类型的安装”界面，如图 1-5 所示。如果选择“升级”选项则进行升级安装，但是若计算机原来没有安装其他操作系统时该项不可用；如果选择“自定义(高级)”则进行全新安装。



图 1-5　选择安装类型界面

(6) 单击“自定义(高级)”选项，进入“您想将 Windows 安装在何处？”界面，该界面显示了当前计算机硬盘的分区信息，如图 1-6 所示。单击“刷新”选项可以重新扫描计算机存储设备，单击“加载驱动程序”可以为 Windows Server 2008 不能直接识别的存储设备安装驱动程序，如 RAID 磁盘阵列，此时仅仅需要将存储有正确驱动程序的 U 盘连接至计算机，并从正确路径选择该驱动程序即可。



图 1-6　分区选择界面

(7) 单击“驱动器选项(高级)”，则可使用安装向导自带的分区工具对当前硬盘进行分区。首先选中“磁盘 0 未分配空间”，然后单击“新建”按钮，输入分区大小，单击“应用”按钮即可，如图 1-7 所示。Windows Server 2008 企业版需要的最小磁盘空间为 10G，但是使用过程中系统文件的大小会逐渐变大，并且还会根据需要添加其他应用程序或数据文件，因此建议为系统分区划分 40G 空间，如果内存较大，由于虚拟内存的关系，可以适当增大系统分区空间。本例中设置为大约 20G 空间。



图 1-7　创建分区界面

(8) 如果还需要为硬盘划分其他分区，可重复上述步骤进行划分，也可划分完系统分区后直接单击“下一步”按钮，先进行系统安装，系统安装完毕后再进行磁盘管理。大多数服务器不会只有一块硬盘，安装好系统后再进行磁盘管理，还可以将所有的硬盘升级为动态磁盘，从而获得更强大的功能，具体操作请参见后面相关章节。如图 1-7 划分好系统分区后，单击“下一步”按钮，打开“正在安装 Windows”界面，开始安装系统，该过程不需要人工干预，如图 1-8 所示。



图 1-8　“正在安装 Windows”界面

(9) 安装过程中，系统会根据需要自动进行重启，不需要人工干预。待安装完毕后，会提示修改管理员密码，如图 1-9 所示。



图 1-9　首次登录界面

(10) 单击“确定”按钮，进入密码更改界面，如图 1-10 所示。Windows Server 2008 系统对密码要求较高，系统管理员帐户必须使用强密码，及必须是大小写字母、数字和其他字符中的 3 种，长度不小于 6 个字符。在密码更改界面中的“新密码”和“确认密码”文本框中分别输入密码，然后按下回车键。



图 1-10　修改密码界面

(11) 如果密码修改成功，则进入如图 1-11 所示的界面。

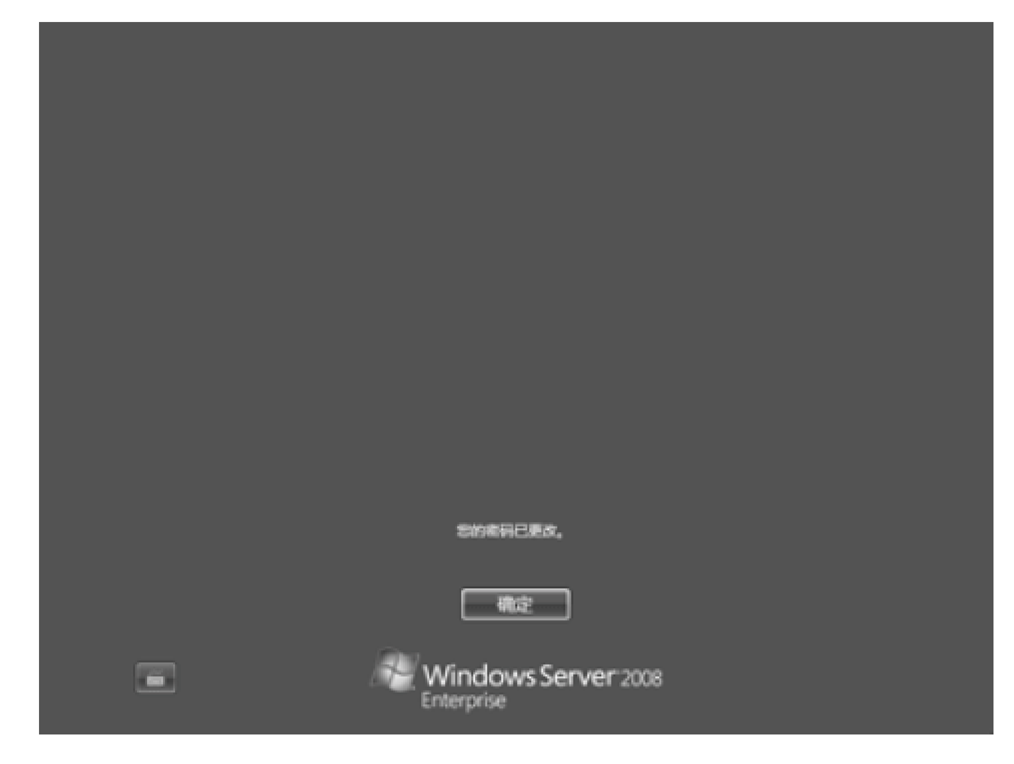


图 1-11　密码修改成功界面

(12) 单击“确定”按钮，等待几分钟后进入操作界面，如图 1-12 所示。



图 1-12　初始桌面

至此，Windows Server 2008 企业版安装完毕。

1.2.4　升级安装

如果服务器上已经有网络服务在运行，而且不能长时间间断，或重新配置会非常复杂，可以考虑使用升级安装模式，将旧版本的 Windows Server 升级到 Windows Server 2008，这样不会使原有的服务长时间中断，也不需要过多地重新对计算机进行设置。但只有 Windows Server 2003 标准版和企业版可以升级至 Windows Server 2008 的标准版和企业版。具体操作步骤如下：

(1) 启动计算机并登录 Windows Server 2003，将 Windows Server 2008 安装光盘放入 DVD 光驱，光驱会自动运行，弹出 Windows Server 2008 安装向导界面，如图 1-13 所示。



图 1-13　安装选项界面

(2) 单击“现在安装”选项，安装向导开始检测计算机配置，如果计算机配置不能满足安装需求，则给出相应提示并终止安装，如果计算机配置可以满足安装需求，则进入“获取安装的重要更新”界面，如图 1-14 所示。



图 1-14　选择安装类型界面

(3) 如果 Windows Server 2003 没有安装过补丁程序或者没有安装最新的补丁程序，可选择“联机以获取最新安装更新(推荐)”选项，这样计算机将连接微软网站，为系统下载并安装最新补丁程序；如果 Windows Server 2003 已经安装最新补丁程序，或至少安装了微软公司为 Windows Server 2003 发布的 SP1 或 SP2 补丁程序包，也可直接单击“不获取最新安装更新”选项，进入“选择要安装的操作系统”界面，如图 1-15 所示。选择准备升级到的 Windows Server 2008 版本。本例选择“Windows Server 2008 Enterprise(完全安装)”，以安装 Windows Server 2008 企业版。

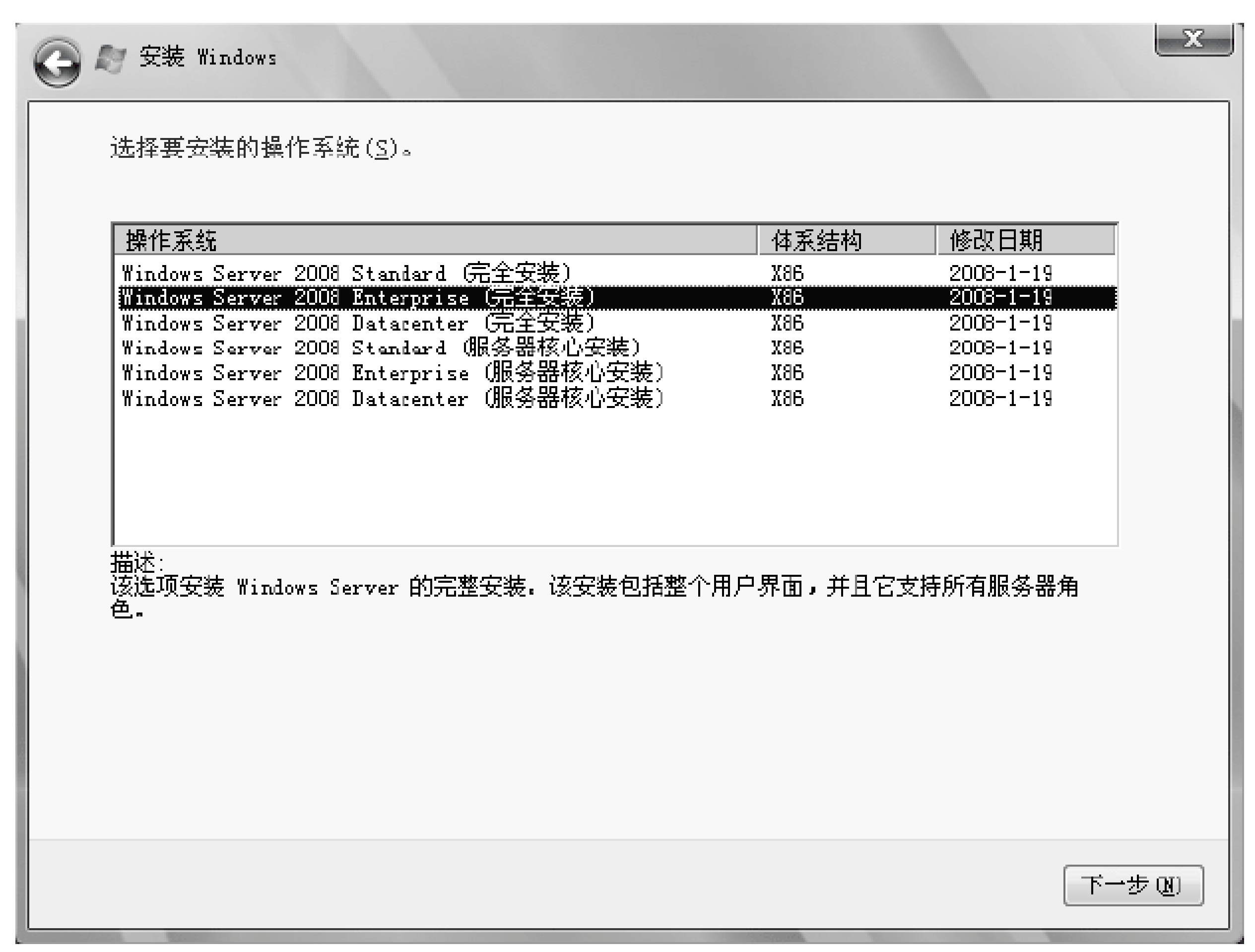


图 1-15　安装版本选择界面

(4) 单击“下一步”按钮，进入“请阅读许可条款”界面，如图 1-16 所示。

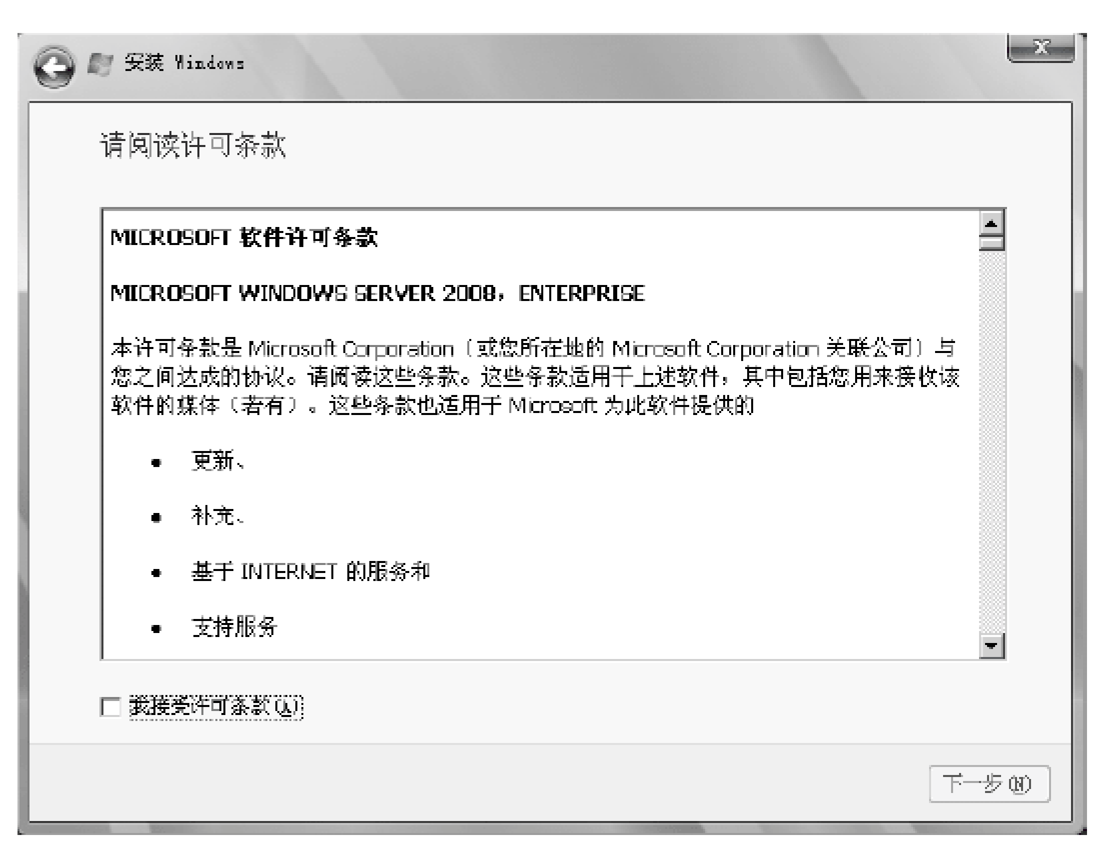


图 1-16　安装协议界面

(5) 选中“我接受许可条款”复选框，单击“下一步”按钮，进入“您想进行何种类型的安装”界面，如图 1-17 所示。



图 1-17　安装类型选择界面

(6) 单击“升级”选项，进入“兼容性报告”界面，如图 1-18 所示。

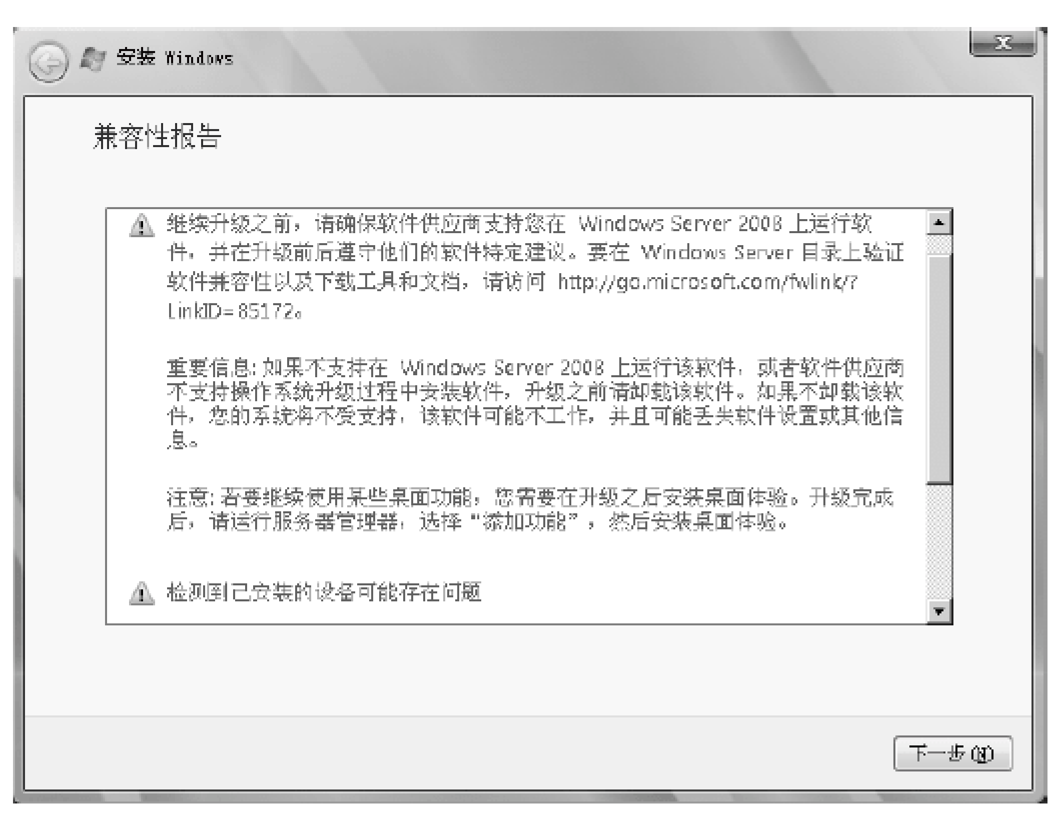


图 1-18　“兼容性报告”界面

(7) 报告会显示出当前计算机的配置是否可以升级到 Windows Server 2008，并列出可能出现的问题。如果报告显示可以升级，单击“下一步”按钮，开始安装系统，步骤和全新安装相同，这里不再赘述。系统安装完毕后，Windows Server 2003 原有的帐户和密码不变，可以使用原有帐户和密码登录系统。

1.3　基本操作

1.3.1　启动和登录

启动和登录是使用 Windows Server 2008 的必经操作，其方法如下：

(1) 打开计算机电源，即可启动 Windows Server 2008，启动后，计算机会暂停于登录界面，如图 1-19 所示。



图 1-19　启动暂停界面

(2) 按下组合键 Crtl+Alt+Delete，即可进入密码输入界面，如图 1-20 所示。



图 1-20　密码输入界面

(3) 输入正确的密码并按下回车键，即可登录到 Windows Server 2008 系统中。

1.3.2　注销与关机

安装系统时设置的密码是为系统管理员帐户而设置的，因此只能以系统管理员身份登录计算机，但很多时候不需要以管理员身份登录，此时可以用普通用户的身份登录服务器。使用其他帐户登录的方式如下：

(1) 单击打开“开始”菜单，如图 1-21 所示。



图 1-21　关机选项

(2) 选择“注销”选项，系统跳转到登录前的界面，按下 Crtl+Alt+Delete 组合键，进入帐户选择界面，如图 1-22 所示。

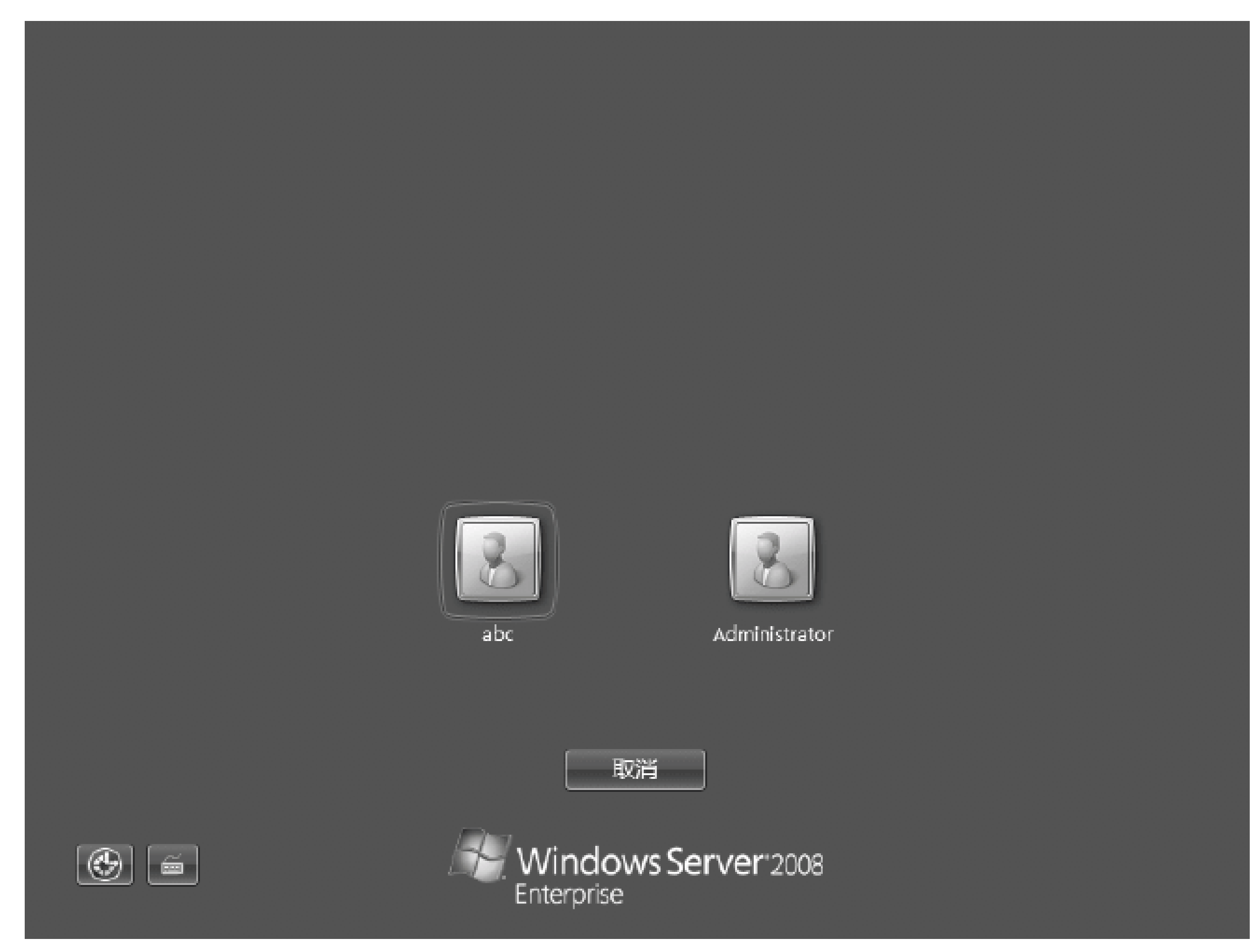


图 1-22　注销登录界面

(3) 单击要进行登录的用户图标，输入正确的密码，按下回车键，即可以该用户帐号登录系统。

Windows Server 2008 是专为网络服务而设计的，因此许多细节之处和普通操作系统是不同的。如关机和重启，网络操作系统一般用于提供不间断的网络服务器，因此每次关机和重启都是应当慎重对待的，Windows Server 2008 要求用户在关机和重启时注明理由以写入日志。操作步骤如下：

(1) 单击“开始”菜单，选择“关机”选项，如图 1-23 所示。



图 1-23　关机选项

(2) 单击“关机”按钮，打开“关闭 Windows”对话框，如图 1-24 所示。



图 1-24　关机理由设置界面

(3) 可在“选项”下拉列表中选择合适的关机理由，如果关机原因不属于菜单中的项目，则可在下方的“注释”文本框中写入关机理由，如图 1-25 所示。



图 1-25　关机理由设置界面

设置完毕后，单击“确定”按钮，完成关机。

重启过程与关机过程类似，这里不再赘述。

1.4 系统基本配置

1.4.1 桌面配置

Windows Server 2008 是一款网络操作系统，主要应用于服务器。因此只要对计算机和网络服务设置完毕后，一般不再对服务器进行设置，因此 Windows Server 2008 的桌面配置不是非常重要。本节介绍 Windows Server 2008 中最常用的分辨率和字体大小选项的设置。操作步骤如下：

(1) 在桌面空白处右击鼠标，在弹出的快捷菜单中选择“个性化”选项，打开“个性化”窗口，如图 1-26 所示，该窗口显示了 Windows Server 2008 中针对桌面可进行的设置。



图 1-26 “个性化和外观”界面

(2) 选择“显示设置”选项，打开“显示设置”对话框，如图 1-27 所示。



图 1-27 “显示设置”对话框

(3) 在该对话框的“分辨率”选项中，可以拖动滑块以调整显示器的分辨率，滑块越向右，分辨率越高，建议使用显示器的最佳分辨率，不要过高也不要过低；“颜色”选项用于设置使用多少种颜色来显示图像，图中显示为“16 位”，表示显示图像时使用 2^{16} 种颜色，这个数值越高，图像色彩越逼真。由于服务器的显示器主要在系统设置时使用，因此没有必要设置得太高。单击“高级设置”按钮，打开“高级设置”对话框，如图 1-28 所示。



图 1-28　监视器设置界面

(4) 选择“监视器”选项卡，可以为显示器设置刷新率。一般来说，CRT 显示器可以设置为 85Hz，LCD 显示器可以设置为 60Hz。设置完毕后单击“确定”按钮即可退出分辨率设置。

(5) 返回到“个性化”窗口，选择“调整字体大小”选项，打开“DPI 缩放比例”对话框，如图 1-29 所示。

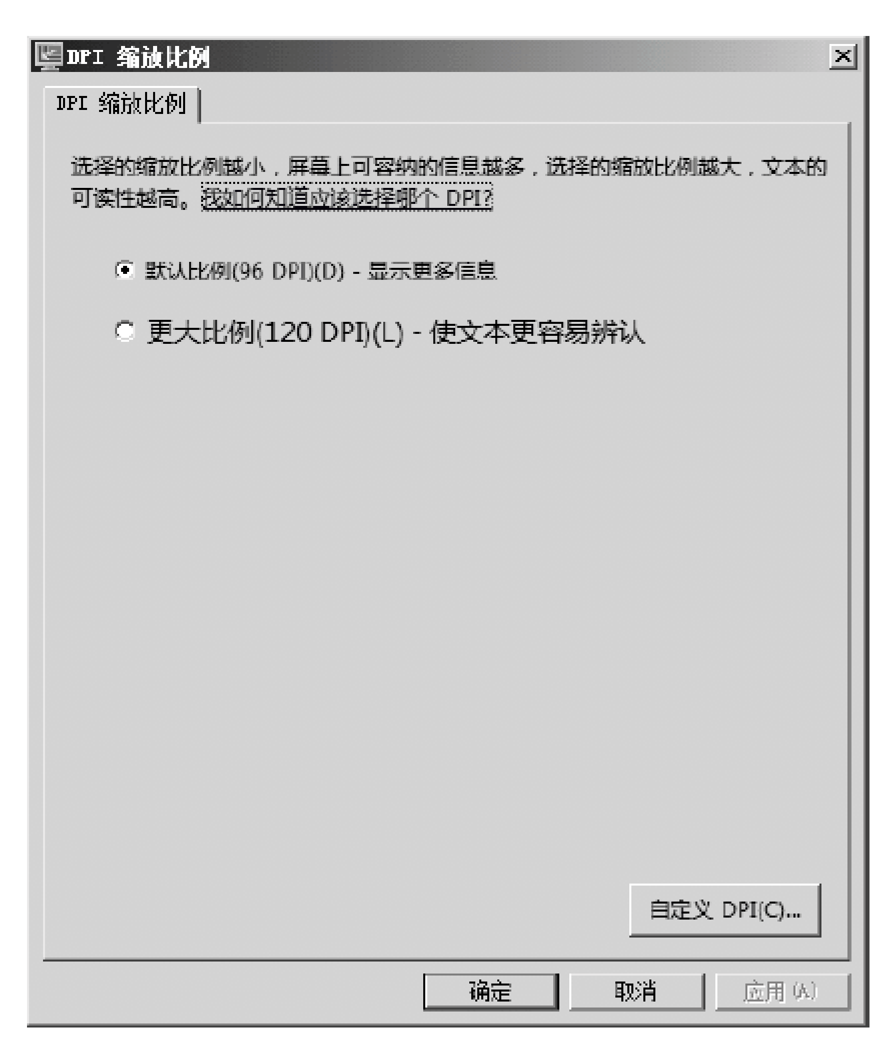


图 1-29　“PPI 缩放比例”对话框

(6) 该对话框可以让用户在不改变分辨率的前提下修改字体大小，以适合自己使用。也可以单击“自定义 DPI”按钮，打开“自定义 DPI 设置”对话框，通过调整百分比来设置文字大小，如图 1-30 所示。

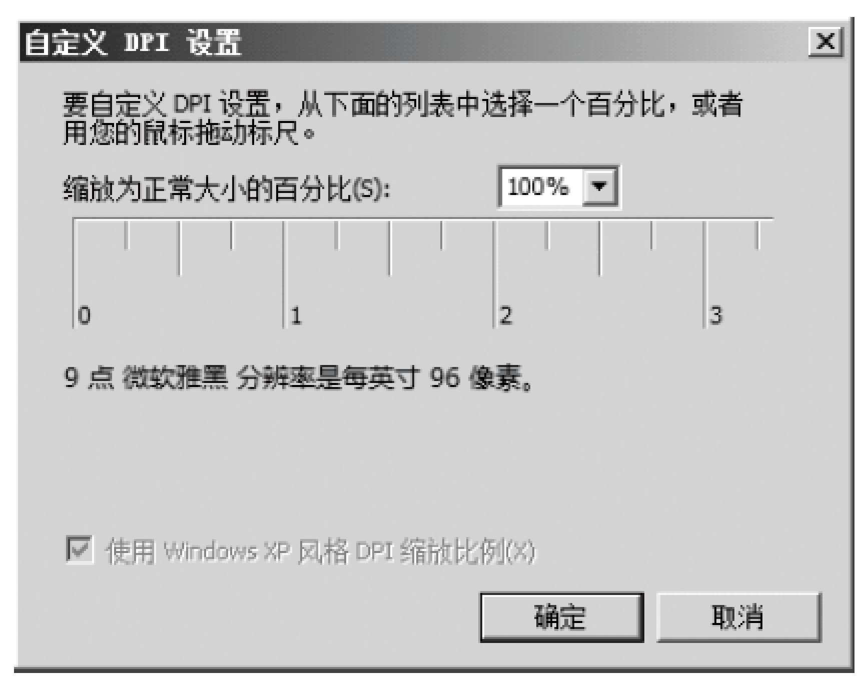


图 1-30　“自定义 DPI 设置”对话框

1.4.2　更改计算机名

Windows Server 2008 的计算机名是系统生成的，如“WIN.UFP0U9E7ZAN”这样的名字，既没有确定含义，也没有什么规律，不便于管理员管理，因此应该按照一定的规律为计算机命名。操作方法如下：

(1) 依次选择“开始”菜单→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口，如图 1-31 所示。



图 1-31　“服务器管理器”窗口

(2) 在右侧窗口中依次选择“服务器摘要”→“计算机信息”→“更改系统属性”命

令，打开“系统属性”对话框，如图 1-32 所示。

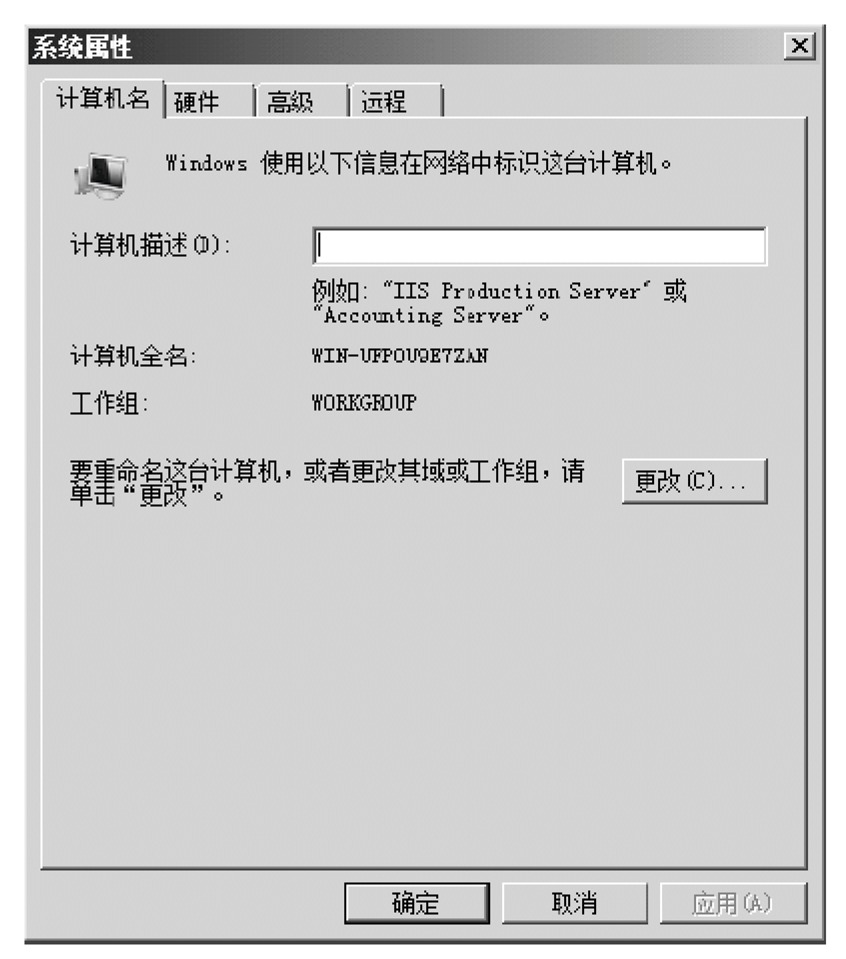


图 1-32　“系统属性”对话框

(3) 在“计算机名”选项卡中可以设置对当前计算机的描述，查看当前计算机的名字和所在工作组，如果当前计算机名需要修改。单击“更改”按钮，打开“计算机名/域更改”对话框，如图 1-33 所示。

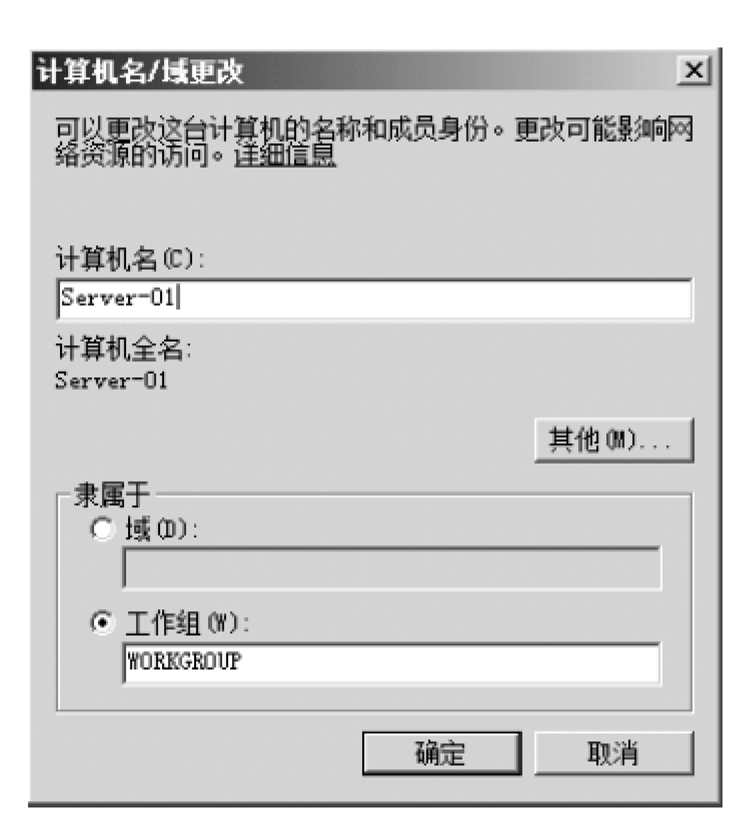


图 1-33　“计算机名/域更改”对话框

(4) 本例中为服务器命名为“Server-01”，如果该服务器在域中，可选中“域”单选按钮，输入所在域的名称；如果该服务器在工作组中，可选中“工作组”单选按钮，输入所在工作组名称。修改完毕后，单击“确定”按钮退出，并根据向导提示重启计算机，即可完成设置。

1.4.3　设置 IP 地址

安装 Windows Server 2008 完毕后，默认通过 DHCP 自动获取 IP 地址，但是这样是有

缺陷的，一是网络内需要有 DHCP 服务器，如果设备提供 DHCP 服务，计算机将无法获取 IP 地址，二是通过 DHCP 服务器分配的 IP 地址是会变化的，不一定可以让同一台计算机每次都获得同一个地址，因此要为服务器设置固定的 IP 地址。具体操作方法如下：

(1) 依次选择“开始”菜单→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口，选择右侧窗口中“服务器摘要”→“计算机信息”→“查看网络连接”命令，打开“网络连接”窗口，如图 1-34 所示。



图 1-34　“网络连接”窗口

(2) 在要配置 IP 地址的网卡的图标上右击，在弹出的快捷菜单中选择“属性”命令，打开该网卡的“属性”对话框，如图 1-35 所示。



图 1-35　“本地连接 属性”对话框

(3) 选择“Internet 协议版本 4(TCP/IP v4)”，再单击“属性”按钮，打开“Internet 协议版本 4(TCP/IPv4)属性”对话框，如图 1-36 所示。

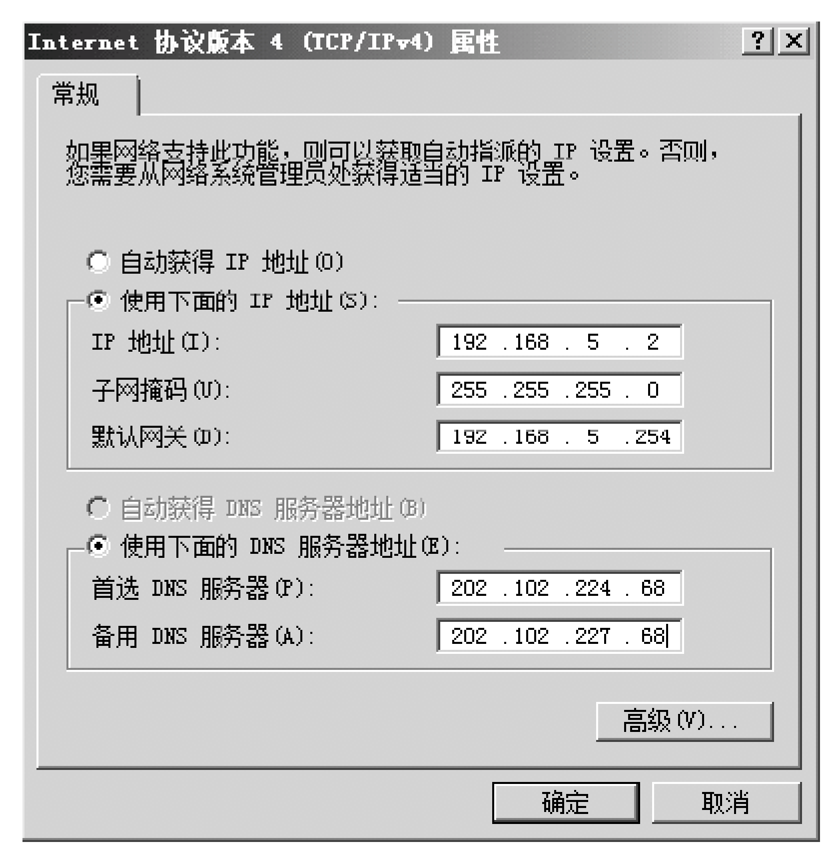


图 1-36　“Internet 协议版本 4(TCP/IPv4)属性”对话框

(4) 选中“使用下面的 IP 地址”单选按钮，即可为服务器输入 IP 地址、子网掩码、默认网关、首选和备用 DNS 服务器地址等配置信息。填写完毕后，单击“确定”按钮，再关闭网卡属性对话框，即可完成配置。

1.4.4　启用 Windows 防火墙

作为一个网络操作系统，其安全性是提供网络服务的保障。如果服务器处于不安全的网络环境中，甚至服务器本身就是不安全的，那么它根本无法保证连续而正确地提供服务。虽然有许多安全解决方案，但是 Windows Server 2008 为加强安全，本身集成有防火墙，本节介绍 Windows Server 2008 的基本防火墙的使用方法，另有高级设置方法，将在后面相关章节中进行介绍。

(1) 打开 Windows Server 2008 的控制面板，双击“Windows 防火墙”图标，打开 Windows 防火墙的设置界面，如图 1-37 所示。



图 1-37　Windows 防火墙设置界面

(2) 单击“更改设置”链接，打开“Windows 防火墙设置”对话框，如图 1-38 所示。

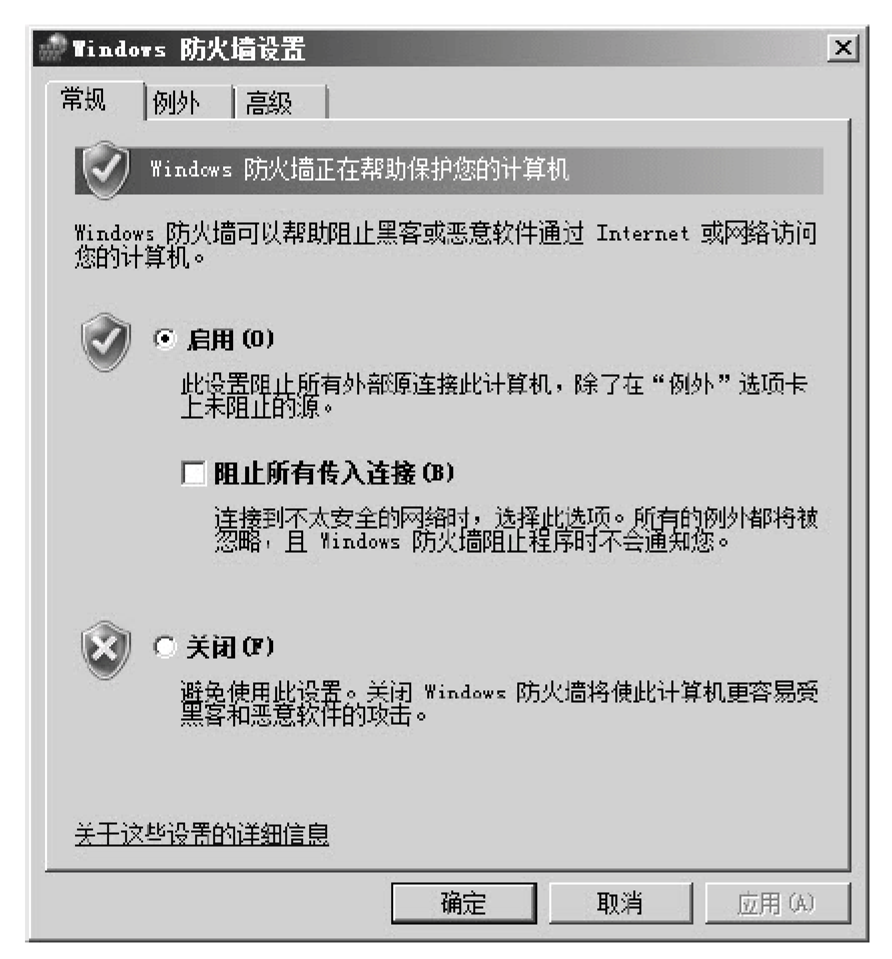


图 1-38　“常规”选项卡

防火墙默认为开启状态，如果不想使用，选中“关闭”单选按钮，然后单击“确定”按钮即可。如果开启了防火墙，“阻止所有传入连接”复选框将可选。选中后，防火墙将阻止所有主动连接该计算机的尝试，但是会放行本机对外的连接，简单来说，外界对本机是无法探测到的。对于个人用户，如果选中该选项，计算机几乎不会被攻击者主动攻击，但作为服务器尽量不要选择这个选项。

(3) 单击打开“例外”选项卡，进入例外配置界面，如图 1-39 所示。

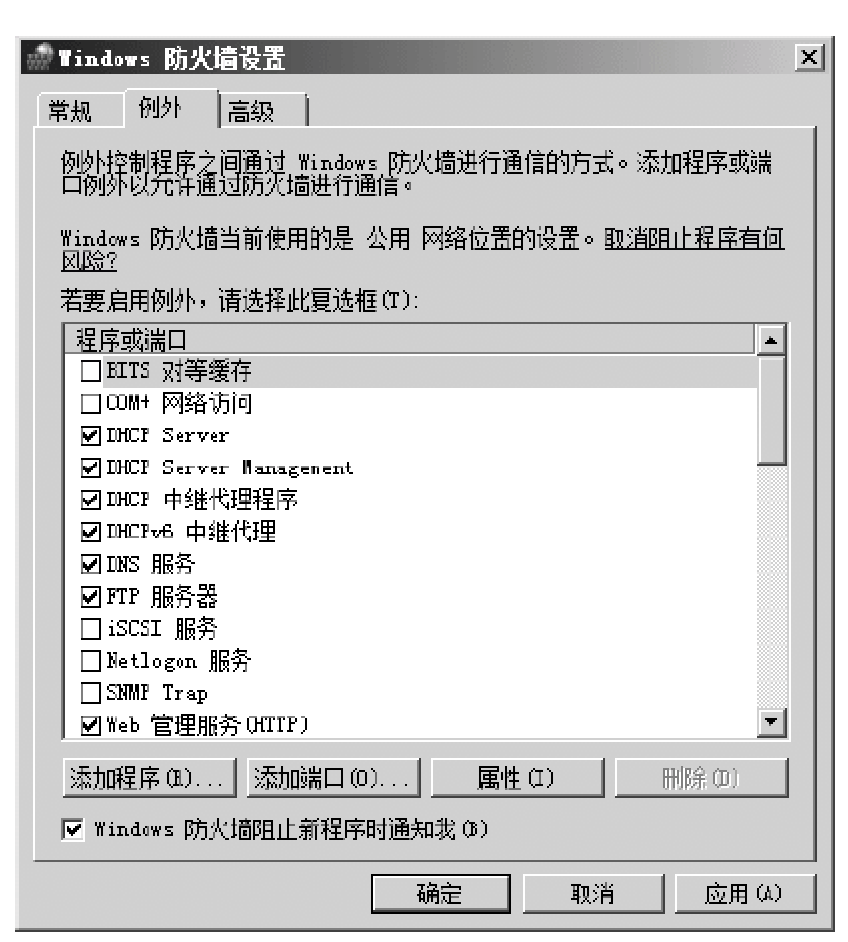


图 1-39　“例外”选项卡

(4) 该界面显示了所有可以通过防火墙的应用程序和端口，被选中的项目就是允许通过防火墙的项目，没有被选中的就是不能通过防火墙的项目。选中某一项后，单击“属性”按钮即可修改其内容；单击“删除”按钮即可删除该例外，使相对应的程序或端口处于禁止通行状态。单击“添加程序”按钮，打开“添加程序”对话框，如图 1-40 所示。



图 1-40　“添加程序”对话框

(5) 在此可以选择“程序”列表框中的程序，或者单击“浏览”按钮选择一个程序所在的路径，单击“确定”按钮后，该程序访问网络时不会被阻止。如果想限定该程序访问网络的范围，则单击“更改范围”按钮，打开“更改范围”对话框，如图 1-41 所示。该对话框有以下 3 个选项：

- 任何计算机：程序可以与所有计算机进行通信。
- 仅我的网络：程序只能和在同一子网内的计算机通信。
- 自定义列表：管理员自定义程序可和那些计算机通信。

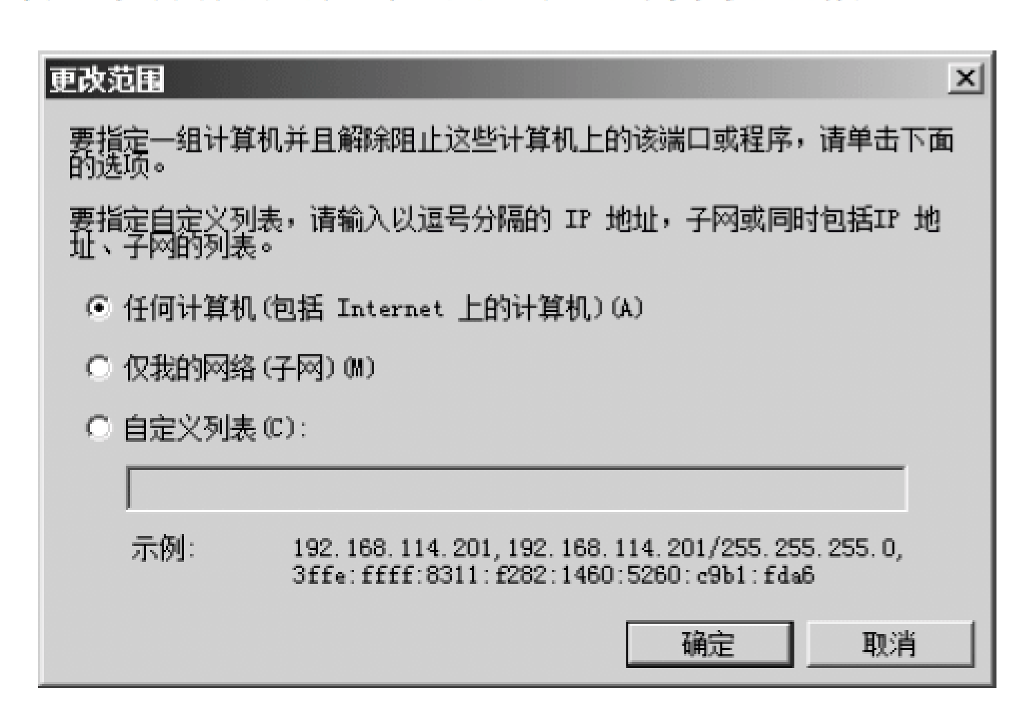


图 1-41　“更改范围”对话框

(6) 设置完毕后，单击“确定”按钮返回“添加程序”界面，再次单击“确定”按钮返回防火墙设置界面。单击“添加端口”按钮，打开“添加端口”对话框，如图 1-42 所示。

(7) 一些服务，如 Telnet 依赖特定端口，因此要使用这类服务必须开放特定的端口。在该对话框中，输入要开放的端口号和名称，选择协议类型，单击“确定”按钮，即可完成配置。“更改范围”按钮和前面相同，这里不再赘述。单击打开“高级”选项卡，进入高级设置界面，如图 1-43 所示。

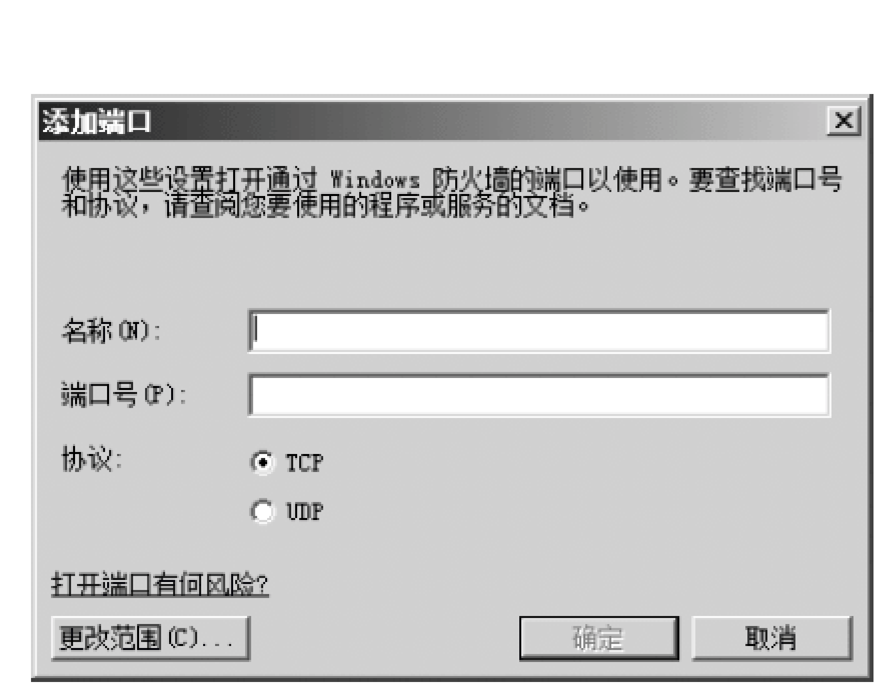



图 1-42　“添加端口”对话框

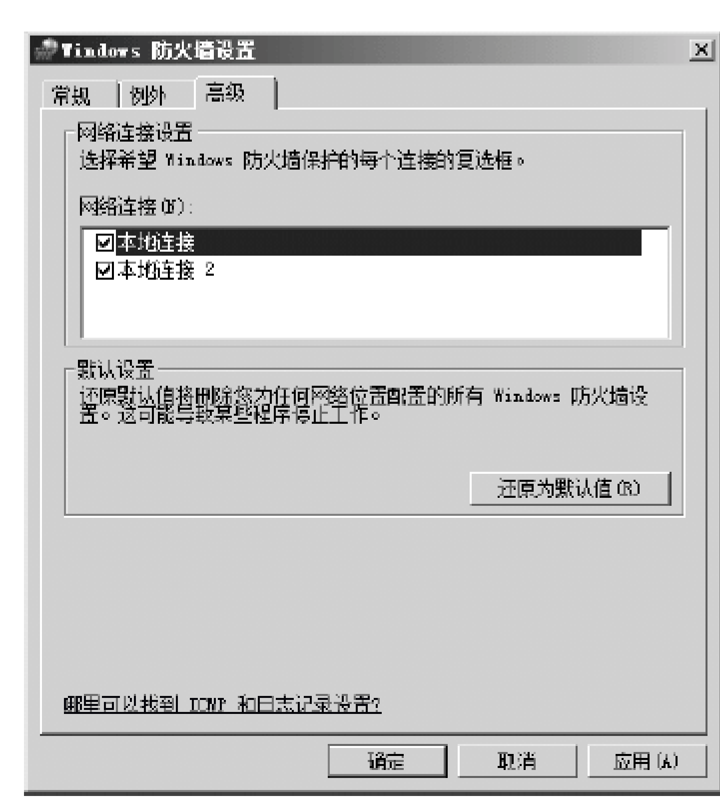


图 1-43　“高级”选项卡

(8) 在该界面中，可以设置哪些网络适配器接受防火墙的保护，哪些不接受防火墙的保护。

1.5　系统的管理

Windows Server 2008 刚安装完毕时是不能提供任何服务的，也就是说，Windows Server 2008 采用的是最小安装策略，用户需要用到什么服务添加即可，这样大大降低了因安装系统服务带来的安全隐患。

Windows Server 2008 将各种服务管理工具高度集成，简化了管理步骤，降低了管理难度。

1.5.1　角色的添加与管理

Windows Server 2008 使用角色的概念来细分服务项目。Windows Server 2008 中管理角色的工具是服务器管理器，具体使用方法如下：

(1) 选择“开始”菜单→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口，然后在左侧窗口中选择“角色”选项，如图 1-44 所示。



图 1-44　“服务器管理器”窗口

(2) 单击“添加角色”，打开“添加角色向导”，如图 1-45 所示。



图 1-45　“添加角色向导”欢迎界面

(3) 选中“默认情况下跳过此页”复选框，单击“下一步”按钮，打开“选择服务器角色”界面，如图 1-46 所示。



图 1-46　“选择服务器角色”界面

(4) 在列表框中选择要安装的服务种类，部分服务可能包含若干项子服务，可以在窗口左侧的“服务器角色”下方的子选项中进一步选择。选择好要安装的服务种类后，单击“下一步”按钮，进入已选中的服务的简介界面中，如图 1-47 所示。



图 1-47　角色详细设置界面

(5) 单击“下一步”按钮，进入“选择角色服务”界面，如图 1-48 所示。

(6) 选择合适的角色，单击“下一步”按钮，进入“确认安装选择”界面，如图 1-49 所示。该界面将前面所选的项目汇总显示出来。

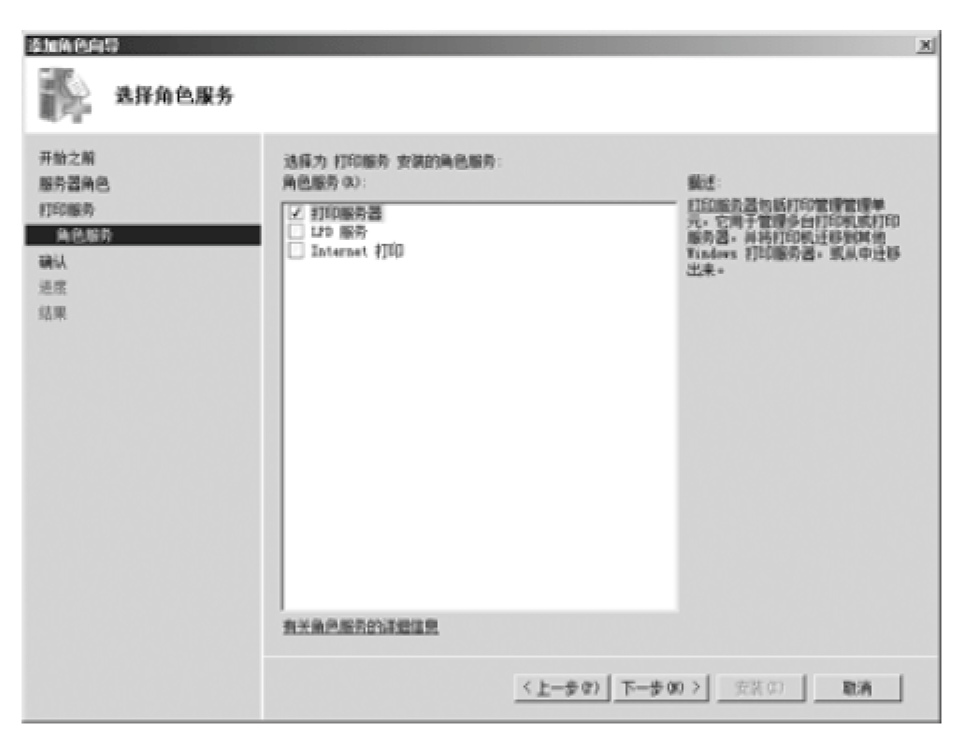




图 1-48　“选择角色服务”界面



图 1-49　“确认安装选择”界面

(7) 如果有需要修改的项目，单击“上一步”按钮返回进行修改；如果不需要作修改，单击“安装”按钮即可开始安装。安装完毕后，显示“安装结果”界面，如图 1-50 所示。



图 1-50　“安装结果”界面

(8) 单击“关闭”按钮即可结束安装。此时返回服务器管理器，管理器中的“角色”一项中已经出现了刚刚安装的服务项目。

安装完毕后，可能需要去掉一些不使用的服务，具体操作方法如下：

(1) 打开服务器管理器，选择“角色”选项，如图 1-51 所示。

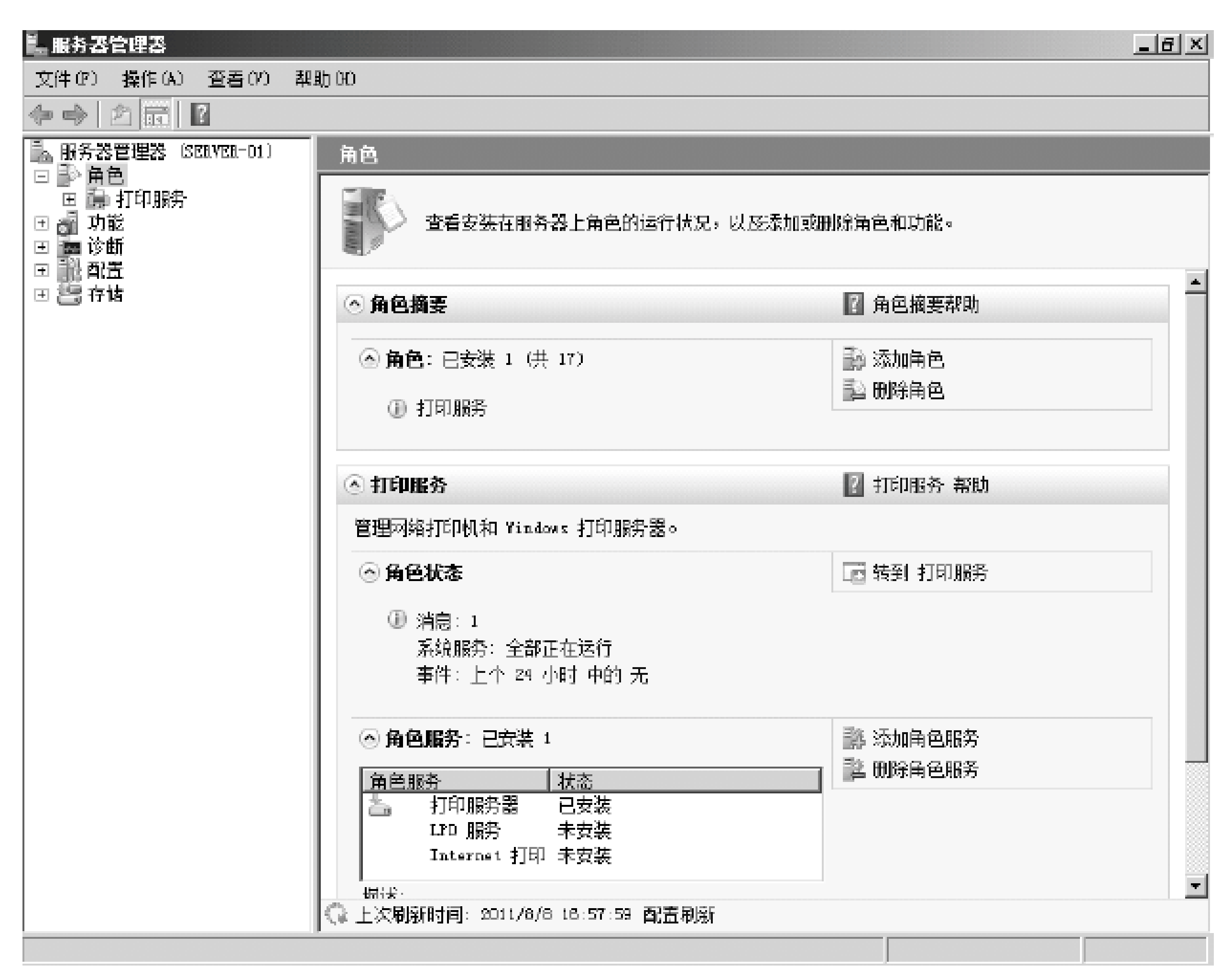


图 1-51　“服务器管理器”界面

(2) 单击“删除角色”，打开“删除角色向导”，如图 1-52 所示。

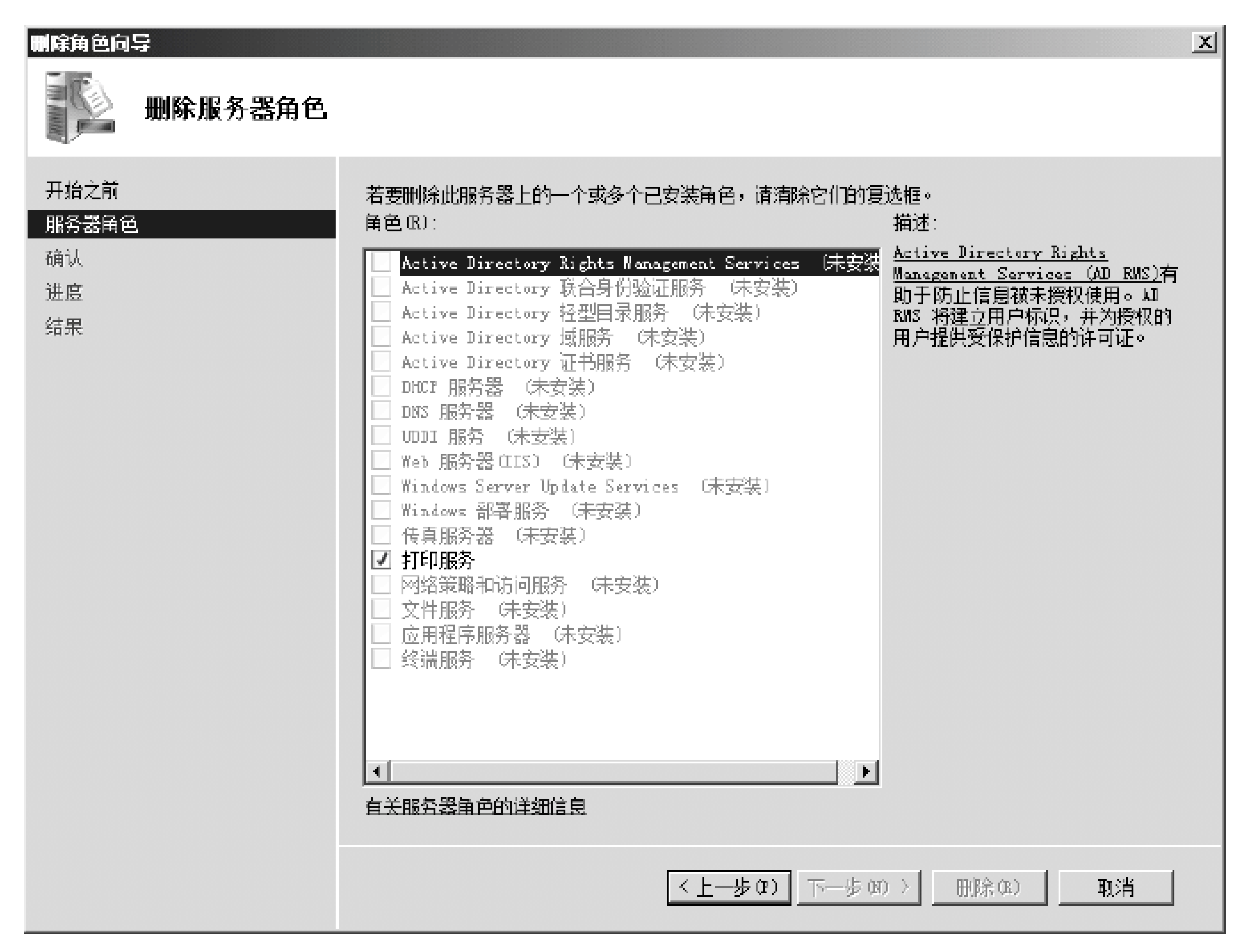


图 1-52　“删除服务器角色”界面

(3) 单击要删除的服务项目，将前面的“√”去掉，然后单击“下一步”按钮，进入详细设置界面，如图 1-53 所示。



图 1-53　删除服务选项界面

(4) 进行设置后，单击“下一步”按钮，进入“确认删除选择”界面，如图 1-54 所示。

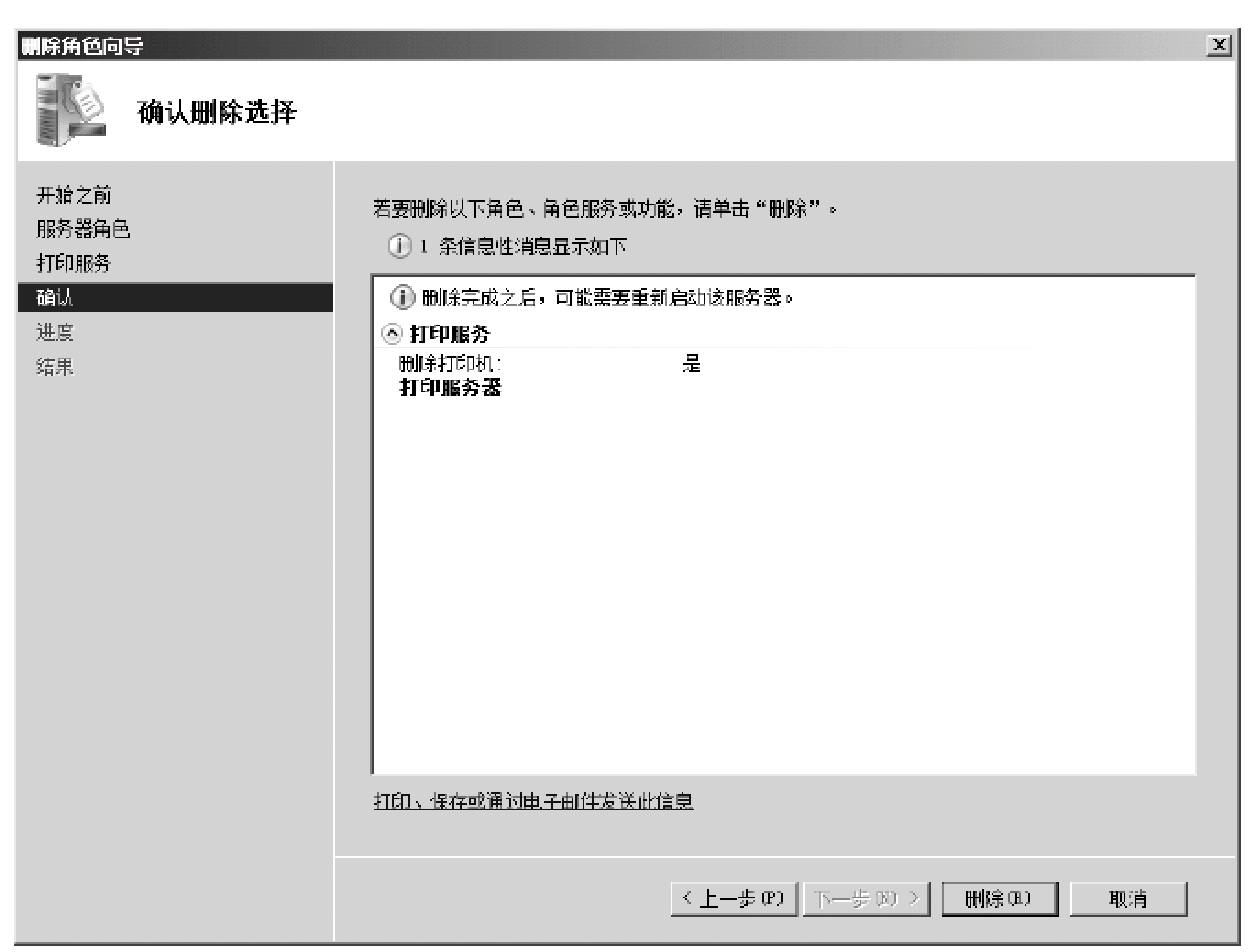


图 1-54　“确认删除选择”界面

(5) 确认无误后，单击“删除”按钮，稍等片刻即可完成删除。

服务器角色是软件程序的集合，在安装并正确配置之后，允许计算机为网络内的多个用户或其他计算机执行特定功能。一般来说，角色具有下列共同特征：角色描述计算机的主要功能、用途或使用。特定计算机可以专用于执行企业中常用的单个角色，如果多个角色在企业中均很少使用，则还可以执行多个角色。角色允许整个组织中的用户访问由其他计算机管理的资源，比如网站、打印机或存储在不同计算机上的文件。角色通常包括自己的数据库，这些数据库可以对用户或计算机请求进行排队，或记录与角色相关的网络用户和计算机的信息。例如，Active Directory 域服务包括一个用于存储网络中所有计算机的名

称和层次结构关系的数据库。正确安装并配置角色之后，将角色设置为自动工作，以允许安装此角色的计算机使用有限的用户命令或管理执行预定的任务。角色服务是提供角色功能的软件程序。安装角色时，可以设置角色将为企业中的其他用户和计算机提供的角色服务。有的角色(例如 DNS 服务器)只有一个功能，因此没有可用的角色服务。其他角色比如终端服务可以安装多个角色服务，这取决于企业的远程计算需要。可以将角色视作对密切相关的互补角色服务的分组，在大多数情况下，安装角色意味着安装该角色的一个或多个角色服务。

功能是一些软件程序，这些程序虽然不直接构成角色，但可以支持或增强一个或多个角色的功能，或增强整个服务器的功能，而不管安装了哪些角色。例如，“故障转移群集”功能增强其他角色(比如文件服务和 DHCP 服务器)的功能，方法是使它们可以针对已增加的冗余和改进的性能加入服务器群集。另一个功能“Telnet 客户端”允许通过网络连接与 Telnet 服务器远程通信，从而全面增强服务器的通信选项。

1.5.2　使用控制台管理系统

Windows Server 2008 集成了控制台功能。通过控制台，可以集中管理原来基于 Web 或单独应用程序等方式的系统工具。控制台的具体操作方法如下：

(1) 依次选择“开始”→“运行”命令，在弹出的对话框中输入 mmc(不含引号)，按下回车键，打开“控制台”窗口，如图 1-55 所示。



图 1-55　“控制台”窗口界面

(2) 依次选择“文件”→“添加/删除管理单元”命令，打开“添加或删除管理单元”对话框，如图 1-56 所示。在“可用的管理单元”列表框中选择需要添加的管理单元，单击“添加”按钮，将所选项目添加到“所选管理单元”列表框中，重复操作可以添加多个管理单元。选择过程中部分管理单元需要声明是管理本机还是管理网络上的其他计算机，用户仅需在提示对话框中选择合适的选项即可。

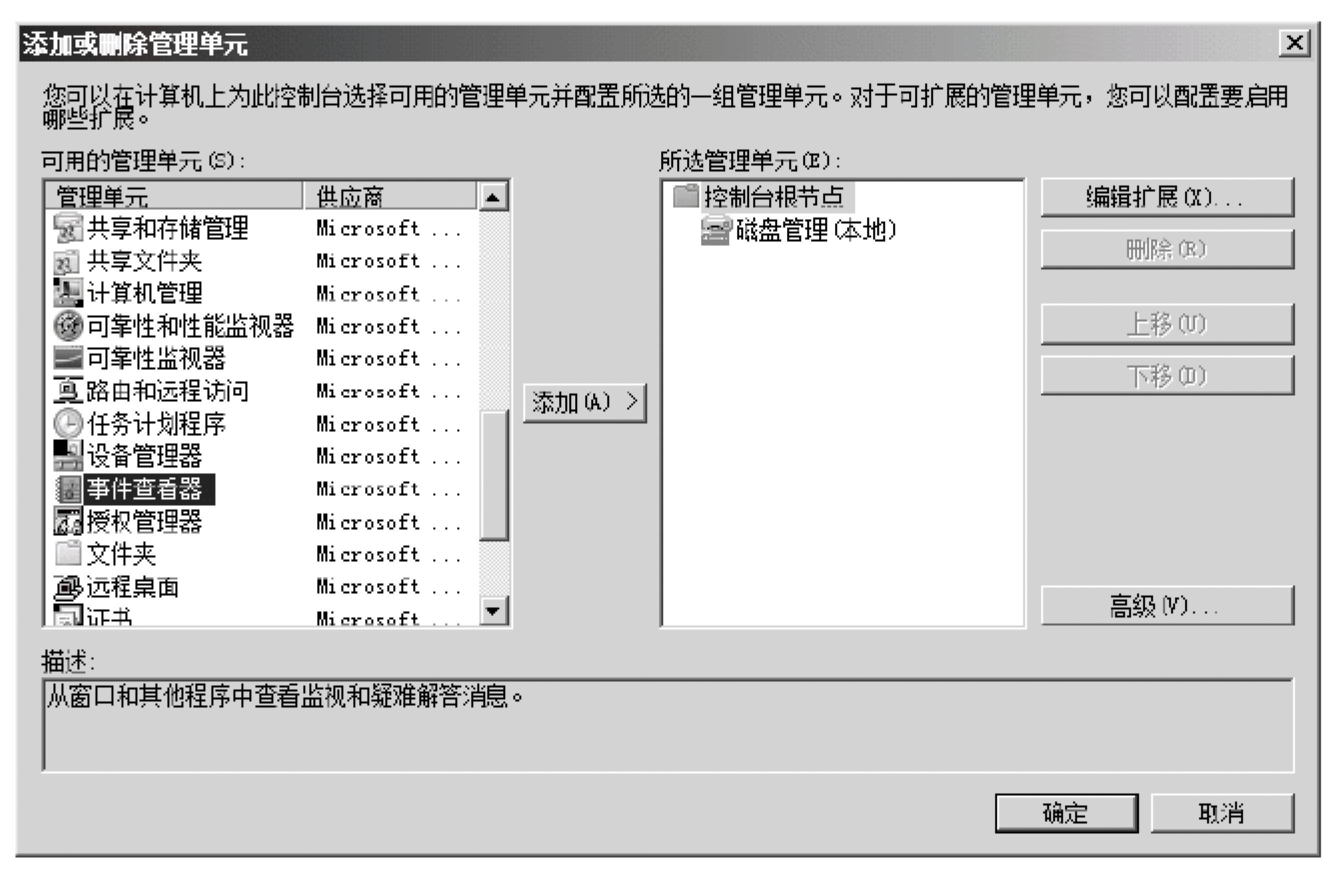


图 1-56　“添加或删除管理单元”对话框

(3) 添加完所需的项目后，单击“确定”按钮，返回控制台，用户可以在控制台中管理刚才所选的项目了。关闭控制台时，系统会提示是否将当前的选择保存起来，如果选择“是”，可以将当前选择保存到“管理工具”中，下次再使用时，依次选择“开始”菜单→“所有程序”→“管理工具”，然后在菜单中找到保存的项目，直接单击即可打开配置好的控制台。

1.5.3　本地用户帐户和用户组

Windows Server 2008 支持多用户，为了保证每个用户能够各司其职，不越权行事，保证系统和资源的安全，管理员应该对每个用户进行权限设置。

一般的系统至少有两类用户，一类是管理员，该类用户具有最高权限，可以设置普通帐户的权限，可以查看所有的文件，可以在系统上执行任何操作而不受限制。管理员中还有一个系统管理员帐户权限在普通管理员之上，可以管理其他普通管理员帐户。另一类是普通用户帐户，该类用户权限较低，往往具有某些权限上的限制，如不能安装软件，或不能删除部分文件，或不能查看其他用户的文件等。

Windows Server 2008 这样的网络服务器操作系统具有的用户更多，如专门设置 IIS 的管理员帐户，专门进行备份操作的管理员帐户等。

为了方便帐户管理，Windows 中提出用户组的概念。管理员可以针对不同的组设置不同的权限，新建帐户后不需要再对帐户逐一进行权限配置，直接将新建的帐户放入相应的组即可。因此能够管理好用户组是一种提高管理效率的做法。

在 Windows Server 2008 中管理组的具体操作方法如下：

(1) 依次选择“开始”菜单→“管理工具”→“计算机管理”命令，接着展开“本地用户和组”选项，如图 1-57 所示。



图 1-57　“计算机管理”窗口

(2) 在“组”选项上右击，在弹出的快捷菜单中选择“新建组”命令，打开“新建组”对话框，如图 1-58 所示。



图 1-58　“新建组”对话框

(3) 在“组名”文本框中输入用户组的名称，此项为必填项；在“描述”文本框中输入对该组的说明，该项为选填。目前该组中还没有任何成员，可以单击“添加”按钮，从弹出的对话框中选择合适的用户添加进该组，或以后在创建或设置用户时再进行添加。设置完毕后，单击“创建”按钮即可完成创建。将所有要添加的组添加完毕后，单击“关闭”按钮关闭对话框。

(4) 如果不再需要某个组，可以在相应的组名上右击，在弹出的快捷菜单中选择“删除”命令，如图 1-59 所示，系统会弹出一个确认对话框，单击“是”按钮即可删除该组。



图 1-59　删除组界面

以上是对组的创建和删除操作。对用户的创建和删除，操作步骤如下：

(1) 打开“计算机管理”工具，并展开“用户和组”选项，在“用户”选项上右击，在弹出的快捷菜单中选择“新用户”命令，打开“新用户”对话框，如图 1-60 所示。

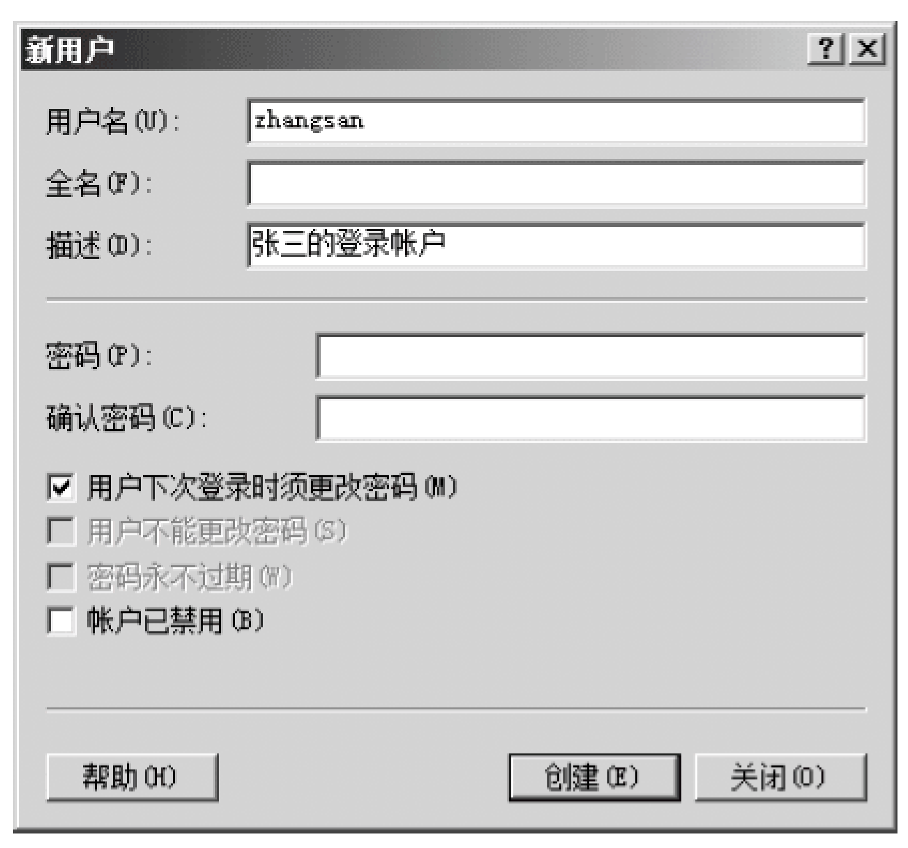


图 1-60　“新用户”对话框

(2) 在对话框中输入相应的信息，每项信息的含义分别如下。

- 用户名：在此处输入标识用户帐户的名称。用户名不能与被管理的计算机上的其他用户名或组名相同。用户名最多可以包含除下列字符外的 20 个大写字符或小写字符：" / \ [ ] : ; | = , + * ? < > @。用户名不能只由句点(.)或空格组成。
- 全名：在此处输入用户的完整名称。最好是建立全名的标准，以便总是以姓(Liang Dawei)或名(Dawei Liang)开头。
- 描述：在此处输入描述用户帐户或用户的任何文本。
- 密码：在此处输入最多 14 个字符的密码。密码区分大小写。
- 确认密码：在此处再次输入密码以确认该密码。
- “用户下次登录时须更改密码”复选框：指定用户下次登录时是否必须更改密码。
- “用户不能更改密码”复选框：指定用户是否能更改分配的密码。通常只在帐户由多个用户使用时才选中该选项，例如，Guest 帐户。此设置对 Administrators 组的成员没有影响。
- “密码永不过期”复选框：指定密码是否永不过期，并忽略组策略的“密码”策略中的“密码最长期限”设置。使用服务分配诸如目录复制器这样的服务时，请选中此选项。此设置将忽略“用户下次登录时须更改密码”。
- “帐户已禁用”复选框：指定是否禁用选定的帐户。

(3) 设置完毕后，单击“创建”按钮即可创建一个新用户。所有的用户都创建完毕后，单击“关闭”按钮即可关闭该对话框，返回到计算机管理工具界面。

(4) 如果某个帐户不需要了，在该帐名上右击，在弹出的快捷菜单中选择“删除”命令，如图 1-61 所示。选择该命令后会弹出一个确认对话框，单击“是”按钮即可删除该用户。



图 1-61　“计算机管理”窗口

(5) 如果在用户名上右击，在弹出的快捷菜单中选择“设置密码”命令，弹出提示对话框，单击“继续”按钮，在弹出的“设置密码”对话框中输入新密码，单击“确定”按钮即可，如图 1-62 所示。

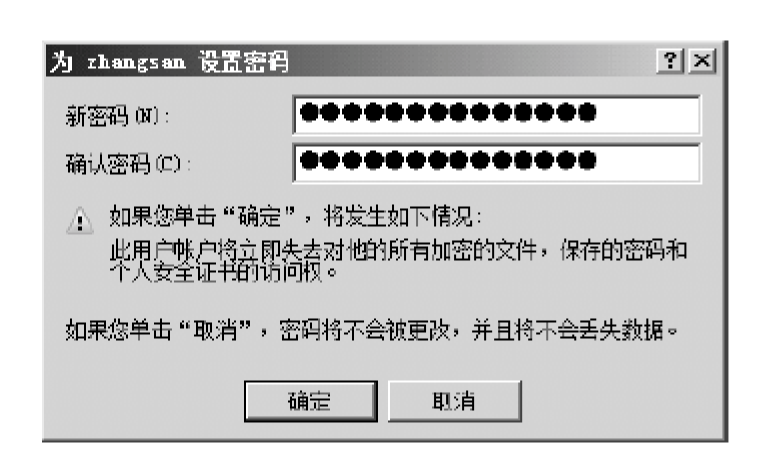


图 1-62　“设置密码”对话框

(6) 如果在用户名上右击，在弹出的快捷菜单中选择“属性”命令，将打开该用户的属性对话框，如图 1-63 所示。



图 1-63　“常规”选项卡

(7) 当前标签栏是用户的基本信息。单击打开“隶属于”选项卡，如图 1-64 所示，可以在其中设置当前用户属于哪个组，从而实现对用户权限的设置。如果想从某个组中删除该用户，选中该组，单击“删除”按钮即可。如果想将用户添加到某个组中，单击“添加”

按钮，从弹出的对话框中选择要添加的组即可。



图 1-64　“隶属于”选项卡

(8) 设置完毕后，单击“确定”按钮退出，返回到计算机管理界面。

1.6　系统启动故障排除

虽然 Windows Server 2008 是目前微软公司稳定性和可靠性最好的操作系统，但是仍然会出现一些故障，较小的故障可以通过重启系统解决，较大的故障则需要重新安装系统。对于一般故障，Windows Server 2008 提供一些启动模式和工具来解决。

1.6.1　启动系统

如果在安装驱动或进行一些设置时 Windows Server 2008 无法正常使用，可以考虑使用“最近一次的正确配置”功能来恢复计算机至正常状态。具体操作方法如下：

(1) 重新启动计算机，在进入系统前按下 F8 键，此时会出现“高级启动选项”界面，如图 1-65 所示。

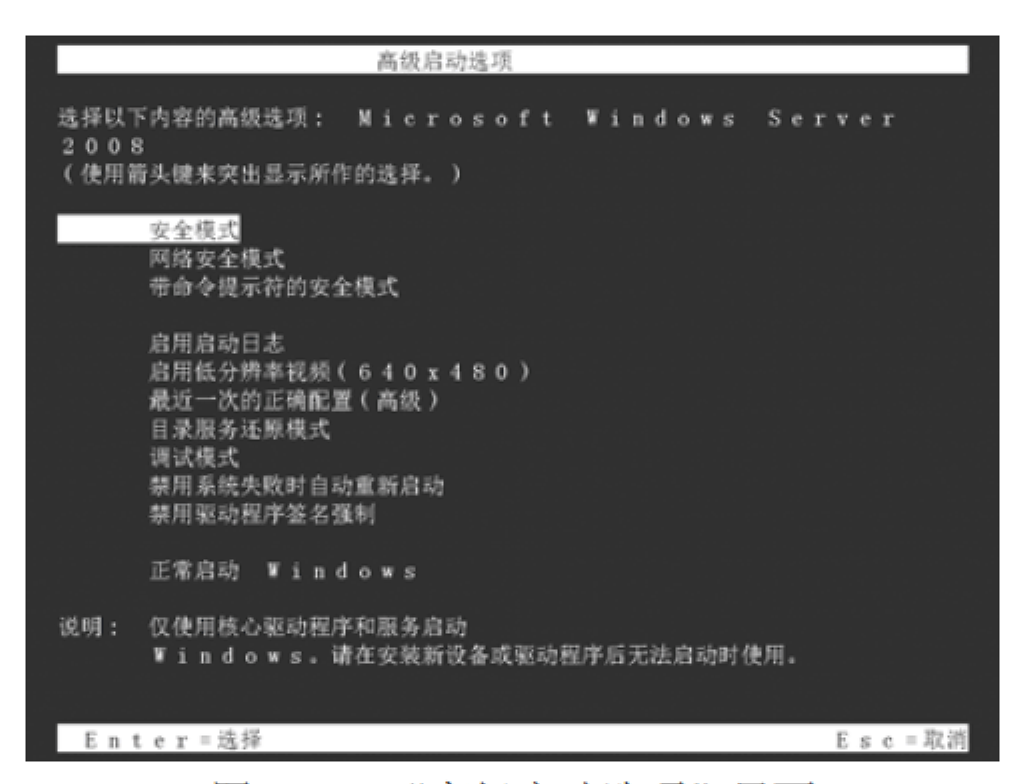


图 1-65　“高级启动选项”界面

(2) 使用上下方向键将光标移至“最近一次的正确配置”选项上，按下回车键即可使用正确配置启动计算机。需要注意的是，该功能并不能正确判断什么样的配置是正确的，什么样的配置是错误的，它仅仅是将最近一次对计算机进行的配置(如升级硬件，更改驱动等)取消，转而使用此前的配置。因此该功能对因为系统文件或驱动程序损坏之类的错误是无法奏效的。如果使用该功能后计算机可以正常使用，则说明最近做的配置和操作中有问题，有利于管理员查找问题所在。但是由于“最近一次的正确配置”功能是取消最近的配置，恢复以前的配置，而且只能恢复注册表项 HKLM\System\CurrentControlSet 中的信息，因此它不是万能的，如果该功能不起作用，则可以尝试“高级启动选项”中的其他模式。

1.6.2　安全模式与其他选项

除了“最近一次的正确配置”，高级启动选项中还有其他选项，这些选项的作用分别如下。

- 安全模式：安全模式是 Windows 的故障排除选项，该模式在限制状态下启动计算机。仅启动运行 Windows 所必需的基本文件和驱动程序。如果计算机以安全模式启动时没有再出现现有问题，用户可以将默认设置和基本设备驱动程序排除在可能的故障原因之外。如果不知道问题的原因，则可以使用排除进程来帮助用户查找问题。尝试启动所有常用程序，包括“启动”文件夹中的程序，依次查看程序是否出现了问题，如果计算机在未出现提示的情况下，自动进入安全模式，则可能是阻止 Windows 正常启动的问题。
- 网络安全模式：在安全模式下启动 Windows，包括访问 Internet 或网络上的其他计算机所需的网络驱动程序和服务。
- 带命令提示符的安全模式：使用安全模式下的命令提示符窗口启动 Windows，而不是通过一般的 Windows 界面启动。此选项适用于 IT 专业人士或管理员。
- 启用启动日志：创建一个 ntbtlog.txt 文件，列出在启动期间安装的所有驱动程序，以及所有可能有助于进行高级故障排除的驱动程序。
- 启用低分辨率视频(640×480)：启动使用当前视频驱动程序和低分辨率以及刷新率设置的 Windows。使用此模式可以重置显示设置。
- 目录服务还原模式：启动运行 Active Directory 的 Windows 域控制器，可以还原目录服务。此选项适用于 IT 专业人士或管理员。
- 调试模式：在专为 IT 专业人士和系统管理员设计使用的高级故障排除模式下，启动 Windows。在此模式下，管理员可以通过串行线路将被调试的计算机的启动信息发送至另一台计算机以便分析。
- 禁用系统失败时自动重新启动：如果错误导致 Windows 启动失败，则阻止 Windows 自动重新启动。仅当 Windows 陷入循环状态时，即 Windows 启动失败，重新启动后再次失败，使用此选项。

- 禁用强制驱动程序签名：允许安装包含了不恰当签名的驱动程序。需要强制安装没有通过微软公司兼容性测试的驱动程序时可以选择此种启动模式，但不建议使用。
- 正常启动 Windows：在正常模式下启动 Windows。

1.6.3　系统的备份与还原

使用高级启动选项只能修复一些简单错误，或作为辅助工具帮助管理员进行故障检测，如果计算机出现了较严重的系统故障，一般的方法是无能为力的，管理员面临的选择可能只有重新安装系统了。但是安装系统耗时较长，尤其是配置服务器耗费的时间更长。如果管理员能够做到经常给系统进行备份，当出现问题时就可以不考虑重新安装系统和重新配置，只需要将正确的备份恢复即可。Windows Server 2008 系统中备份与还原的具体操作方法如下：

(1) Windows Server 2008 在默认状态下没有安装备份工具，需要管理员手工添加。打开服务器管理器，选择左侧窗口中的“功能”选项，再单击右侧窗口中的“添加”选项，打开“添加功能”向导，如图 1-66 所示。

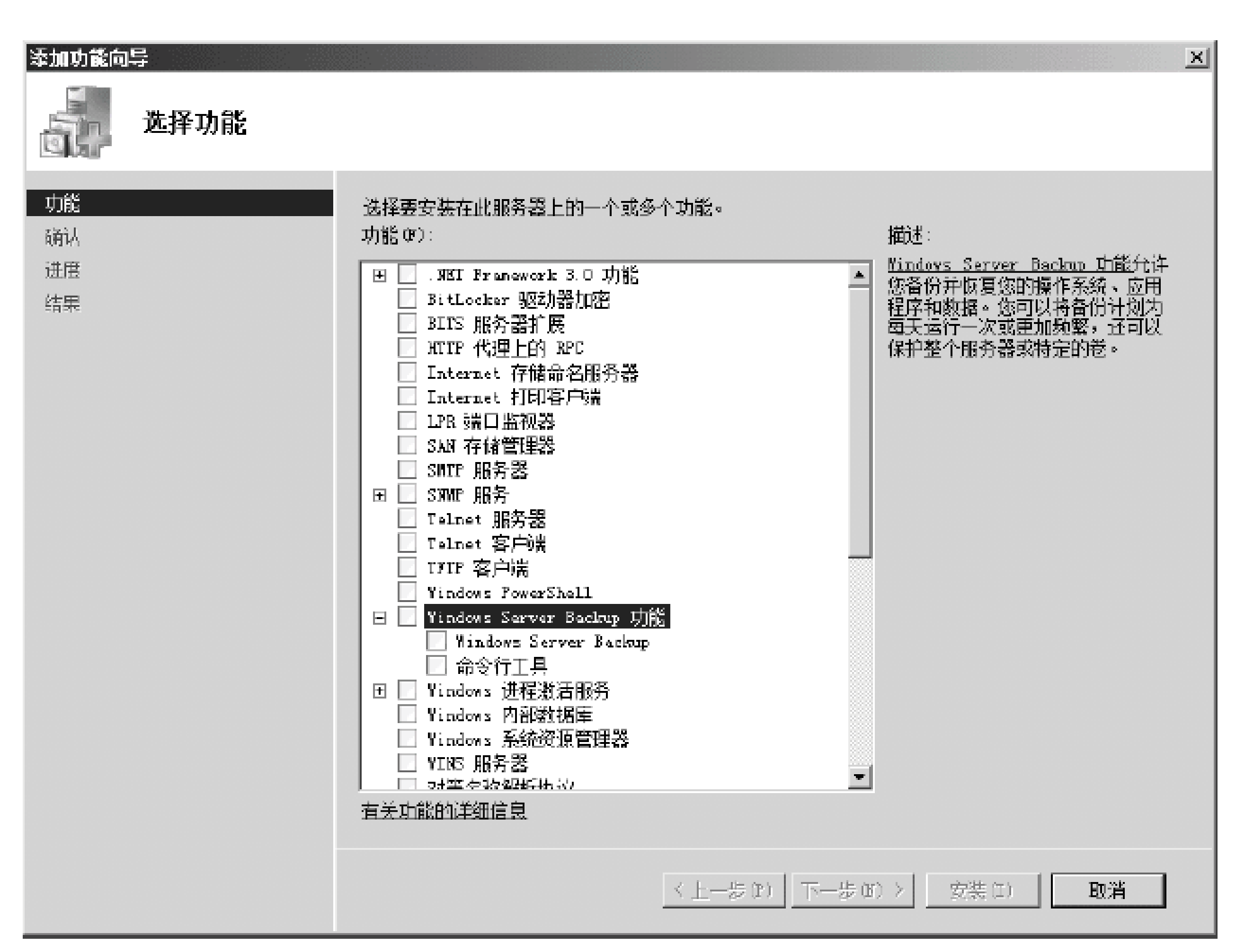


图 1-66　“选择功能”界面

(2) 选中其中的“Windows Server Backup 功能”，该功能有两个子功能，其中“Windows Server Backup”已经可以满足基本要求，“命令行工具”则允许管理员在命令行中使用命令对系统进行备份和恢复。本例中只选择“Windows Server Backup”，这也是“Windows Server Backup 功能”的默认选项。选择完成后单击“下一步”按钮，根据向导提示即可完成安装。具体步骤与添加角色类似，这里不再赘述。

(3) 安装完毕后，依次选择“开始”菜单→“管理工具”→“Windows Server Backup”命令，打开备份工具窗口，如图 1-67 所示。



图 1-67　“Windows Server Backup”界面

(4) 单击“一次性备份”选项，打开一次性备份向导，如图 1-68 所示。

(5) 目前还没有设置备份计划，因此只能选择“不同选项”，单击“下一步”按钮，进入“选择备份配置”界面，如图 1-69 所示。

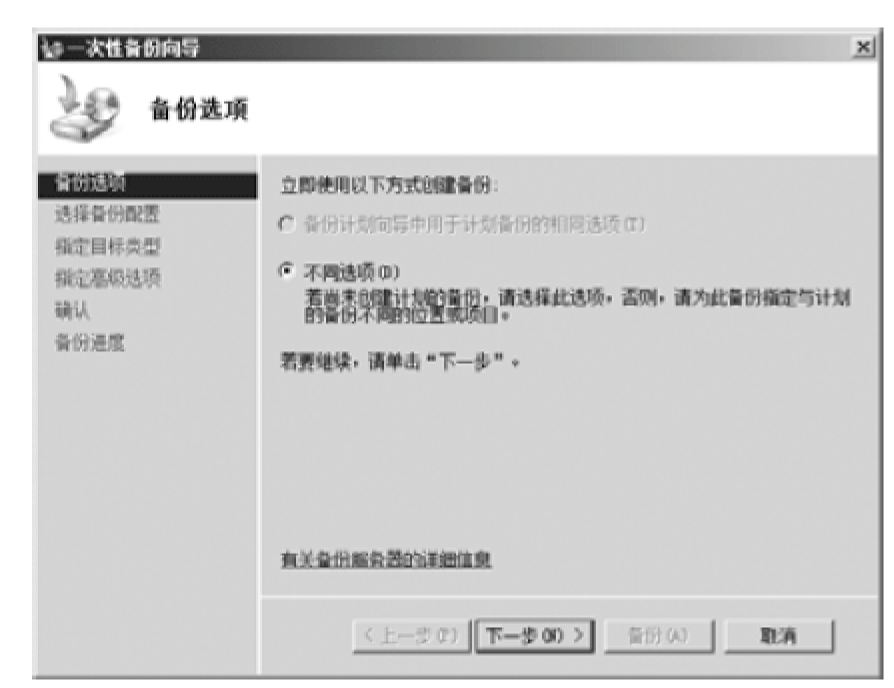


图 1-68　“备份选项”界面

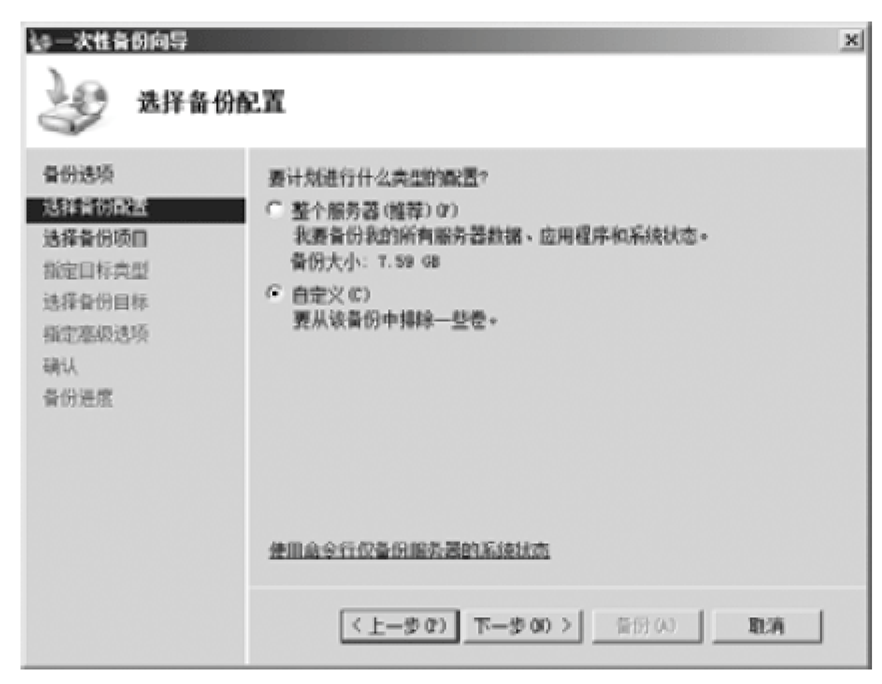


图 1-69　“选择备份配置”界面

(6) 本界面有两个选项，选中“整个服务器”选项则将备份服务器上所有的内容，适合第一次做备份，但是备份内容多，信息量大，而且最好另准备一块硬盘专门用于备份；选中“自定义”选项则备份指定的卷(Windows Server 2008 的磁盘管理器中没有分区的概念，可以将卷看作是功能更强大的分区，后面章节会有详细介绍)。本例中选择“自定义”，然后单击“下一步”按钮，进入“选择备份项目”界面，如图 1-70 所示。

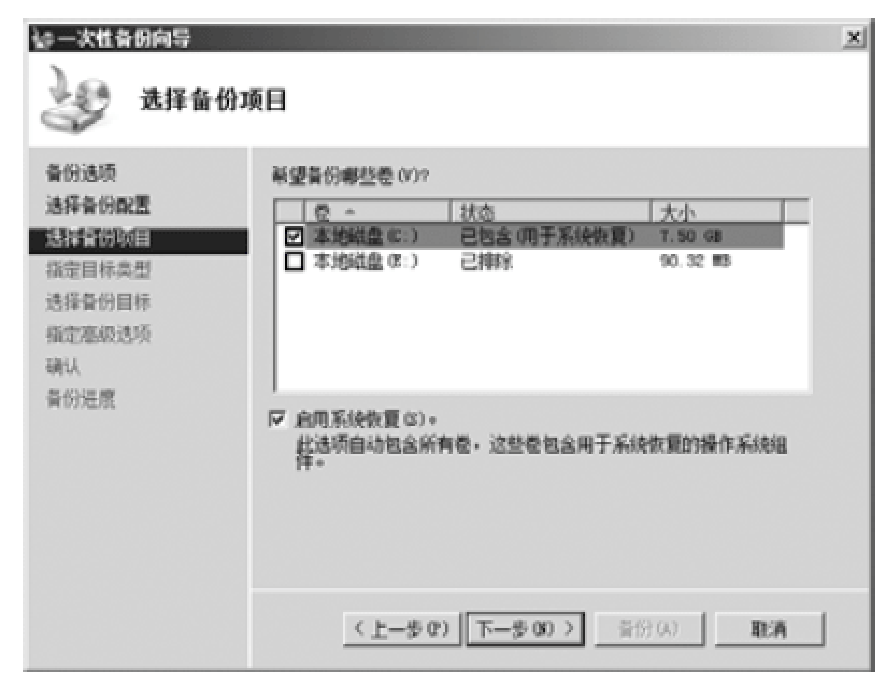


图 1-70　“选择备份项目”界面

(7) 在“希望备份哪些卷？”列表框中选中要备份的卷，取消不备份的卷，单击“下一步”按钮，进入“指定目标类型”界面，如图 1-71 所示。



图 1-71　“指定目标类型”界面

(8) 在本界面中可以选择将备份文件保存于本地硬盘还是网络空间中，本例选择“本地驱动器”选项，如果选择“远程共享文件夹”则可将备份文件保存于其他计算机的共享文件夹中，前提是两台计算机必须网络通畅并设置了合适的权限。单击“下一步”按钮，进入“选择备份目标”界面，如图 1-72 所示。

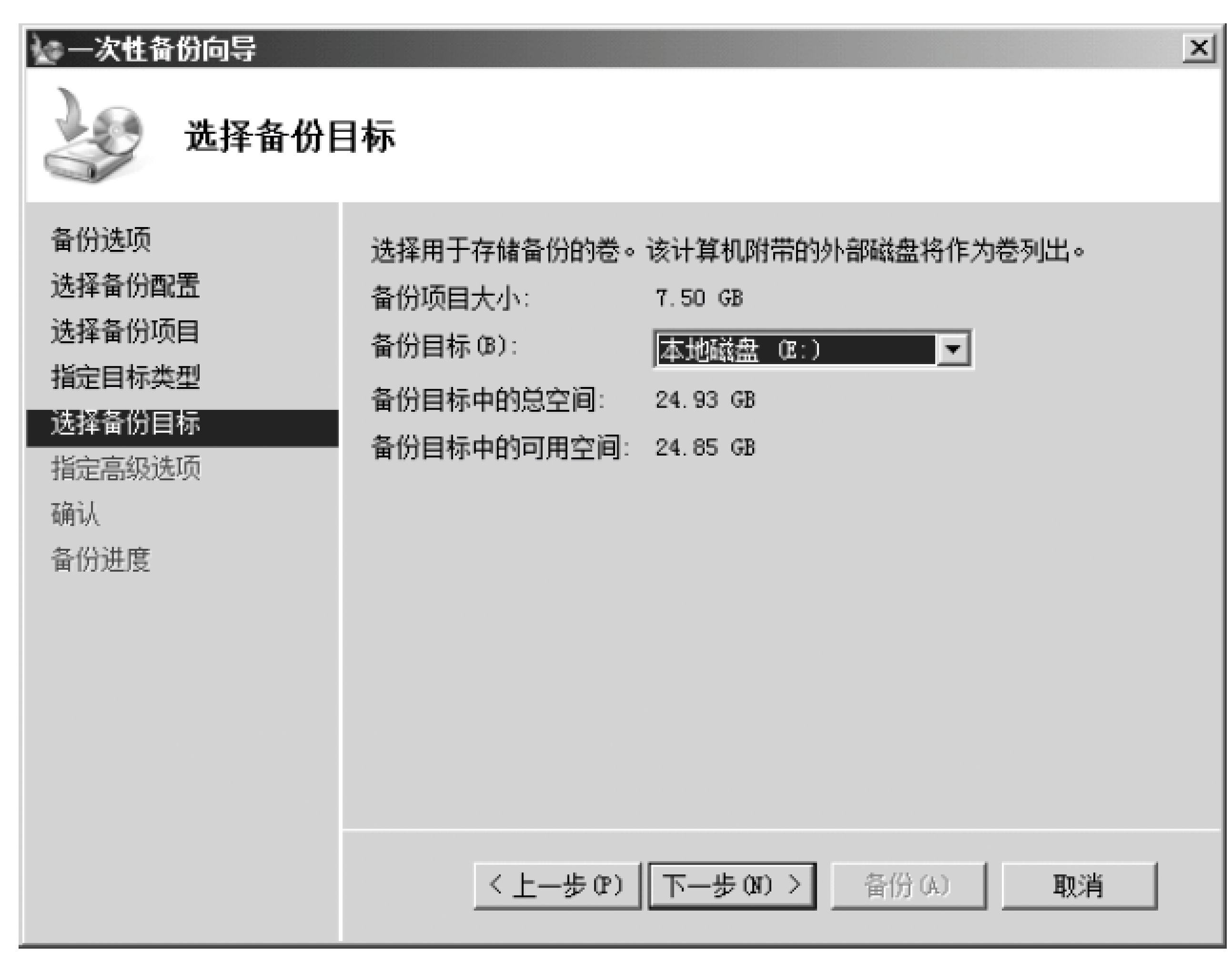


图 1-72　“选择备份目标”界面

(9) 本界面用于选择将备份文件保存于哪个卷中，可以在“备份目标”下拉列表中选择，选择完毕后单击“下一步”按钮，进入“指定高级选项”界面，如图 1-73 所示。

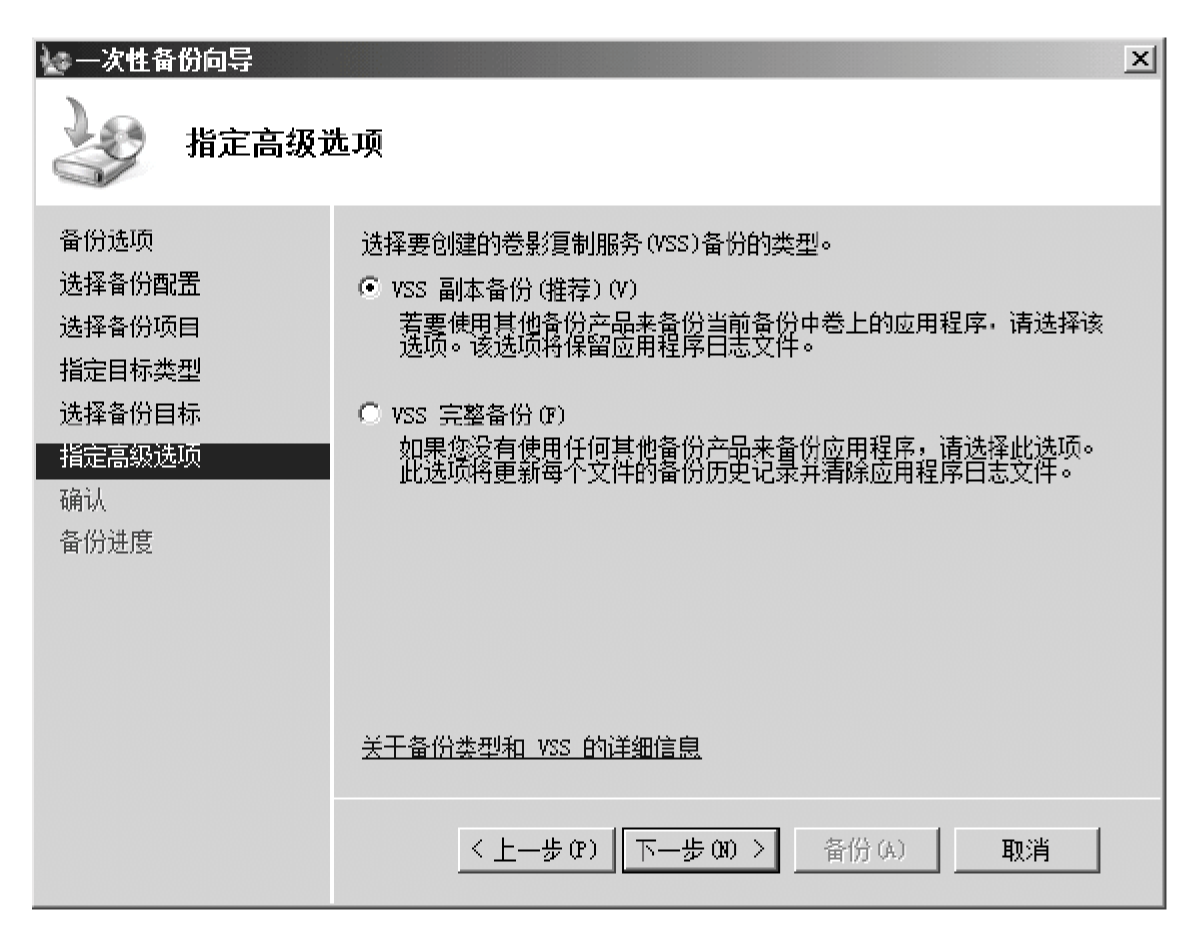


图 1-73　“指定高级选项”界面

(10) 如果管理员使用其他方式对系统进行备份，则选择“VSS 副本备份(推荐)”，如果没有使用其他方式对系统进行备份，则选择“VSS 完整备份”。两者的最大区别在于如何对待系统中的应用程序。选择完毕后，单击“下一步”按钮，进入“确认”界面，如果对当前设置满意不再需要修改，则单击界面中的“备份”按钮，等待几分钟后，备份完成。

(11) Windows Server 2008 提供了两种备份模式。在“Windows Server Backup”管理界面右侧选择“配置性能设置”选项，打开“优化备份性能”对话框，如图 1-74 所示。

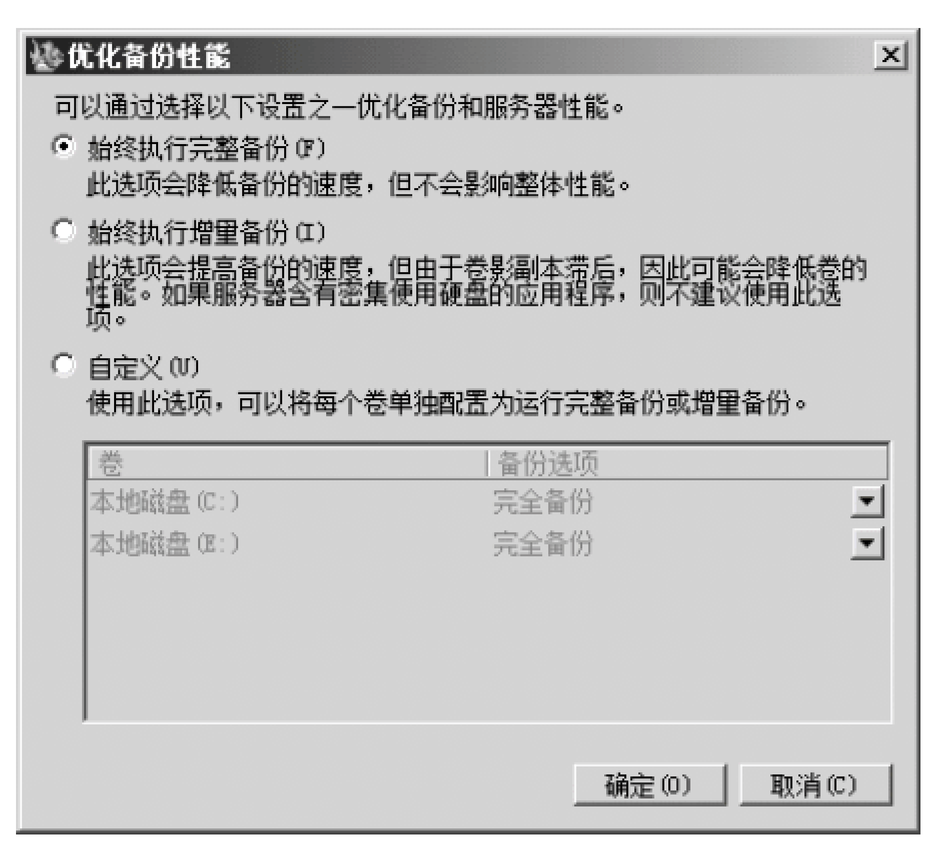


图 1-74　“优化备份性能”对话框

(12) Windows Server 2008 中的两种备份模式，一是完整备份模式，该模式下备份工具将备份系统中所有的信息，备份内容完整，但是信息量大，占用磁盘空间较大，一般用于对系统的第一次备份；二是增量备份模式，该模式下备份工具只备份自上次备份后系统修改的部分，备份内容少，但是信息量小，占用磁盘空间较少，一般用于完整备份后系统再被更改的备份。管理员可以根据需要，适当设置“优化备份性能”对话框中的选项。选择完毕后，单击“确定”按钮，下次备份时设置生效。

(13) Windows Server 2008 还提供了自动备份的功能。在“Windows Server Backup”管理界面中选择“备份计划”选项，打开备份计划向导，如图 1-75 所示。

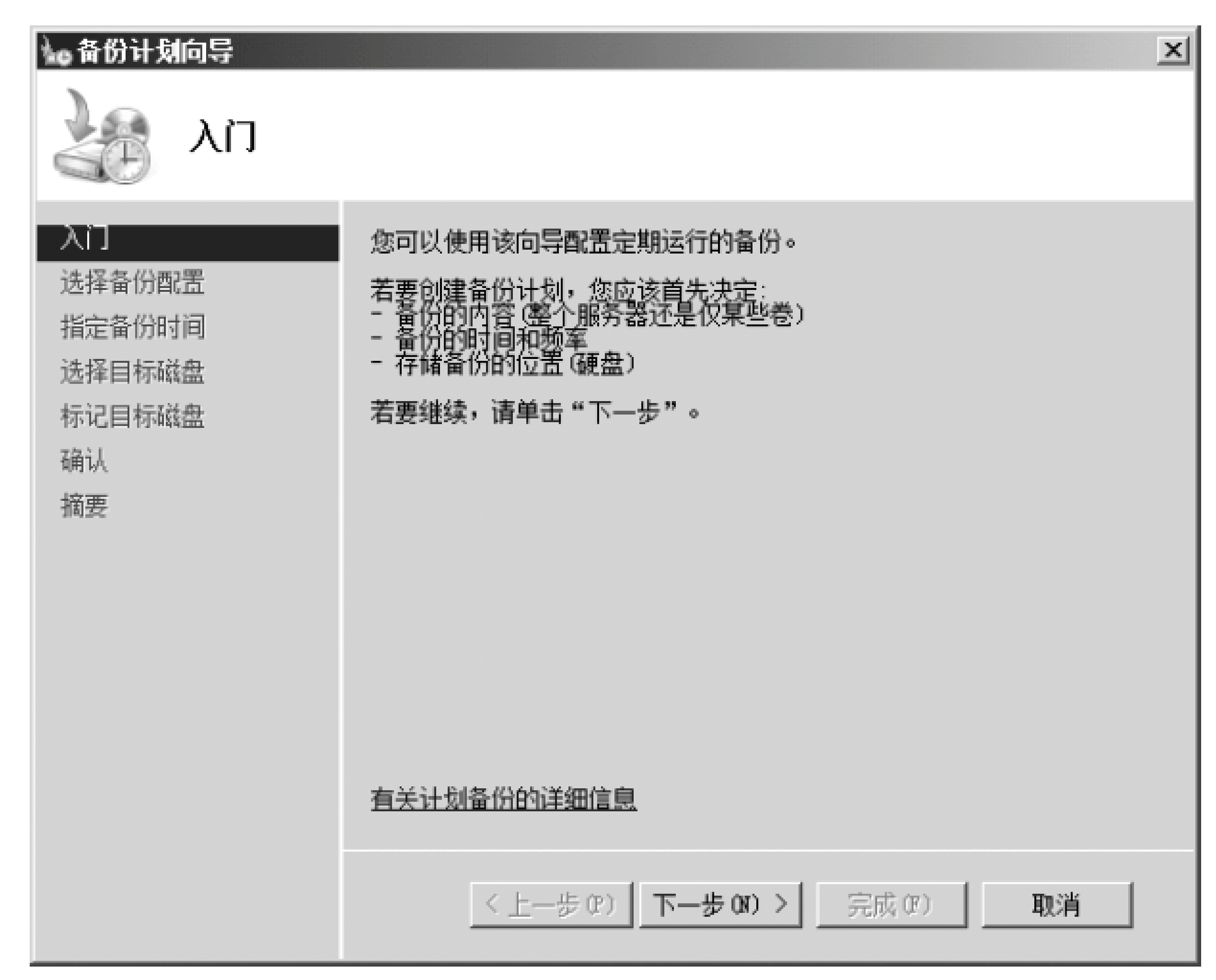


图 1-75　备份计划向导欢迎界面

(14) 单击“下一步”按钮，进入“选择备份配置”界面，如图 1-76 所示。在该界面中设置是对整个服务器进行备份还是只对某些卷进行备份。如果选择了“自定义”选项，还要指定要备份的卷。

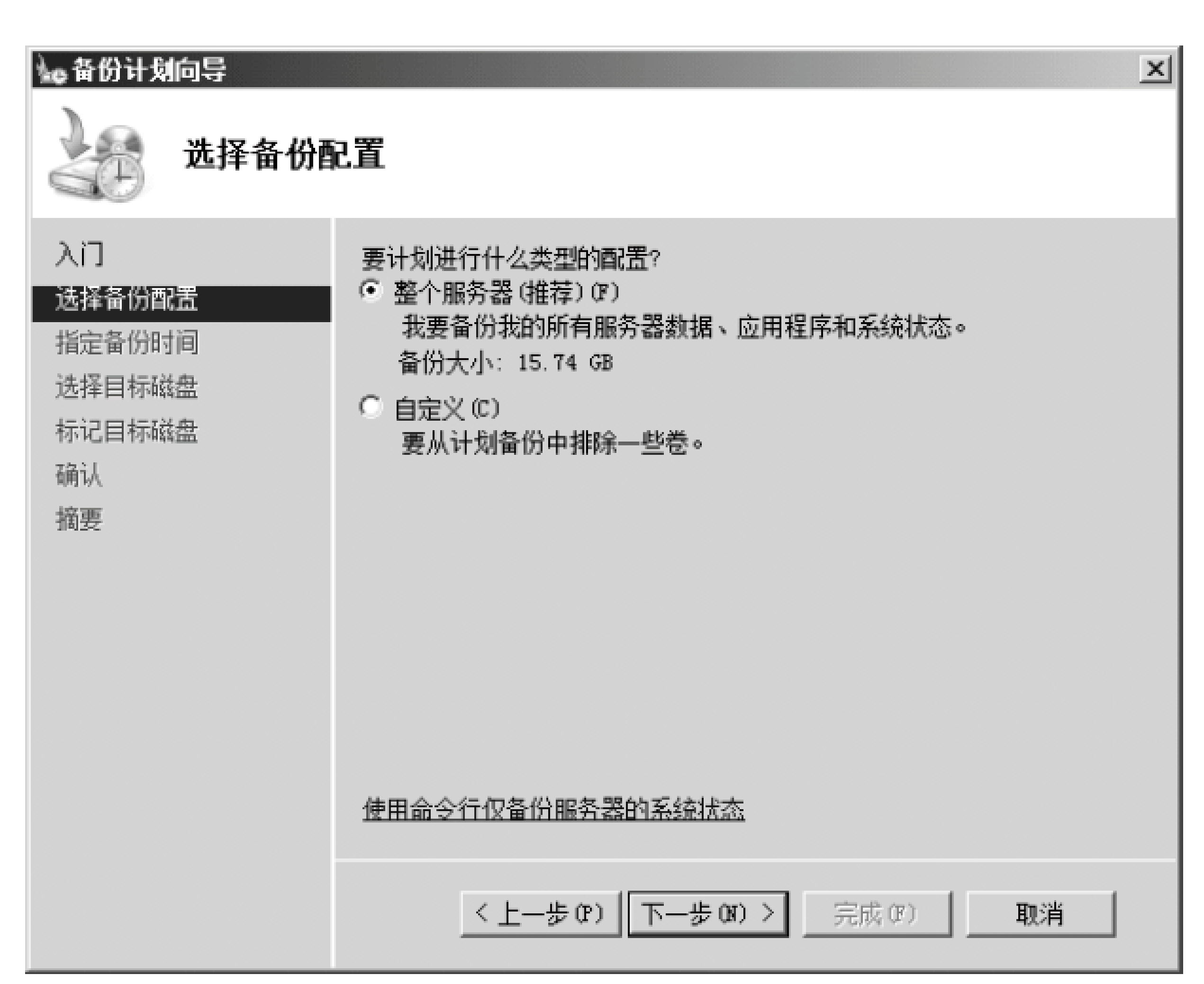


图 1-76　“选择备份配置”界面

(15) 选择完毕后，单击“下一步”按钮，进入“指定备份时间”界面，如图 1-77 所示。在该界面中可以选择以什么样的频率进行自动备份。

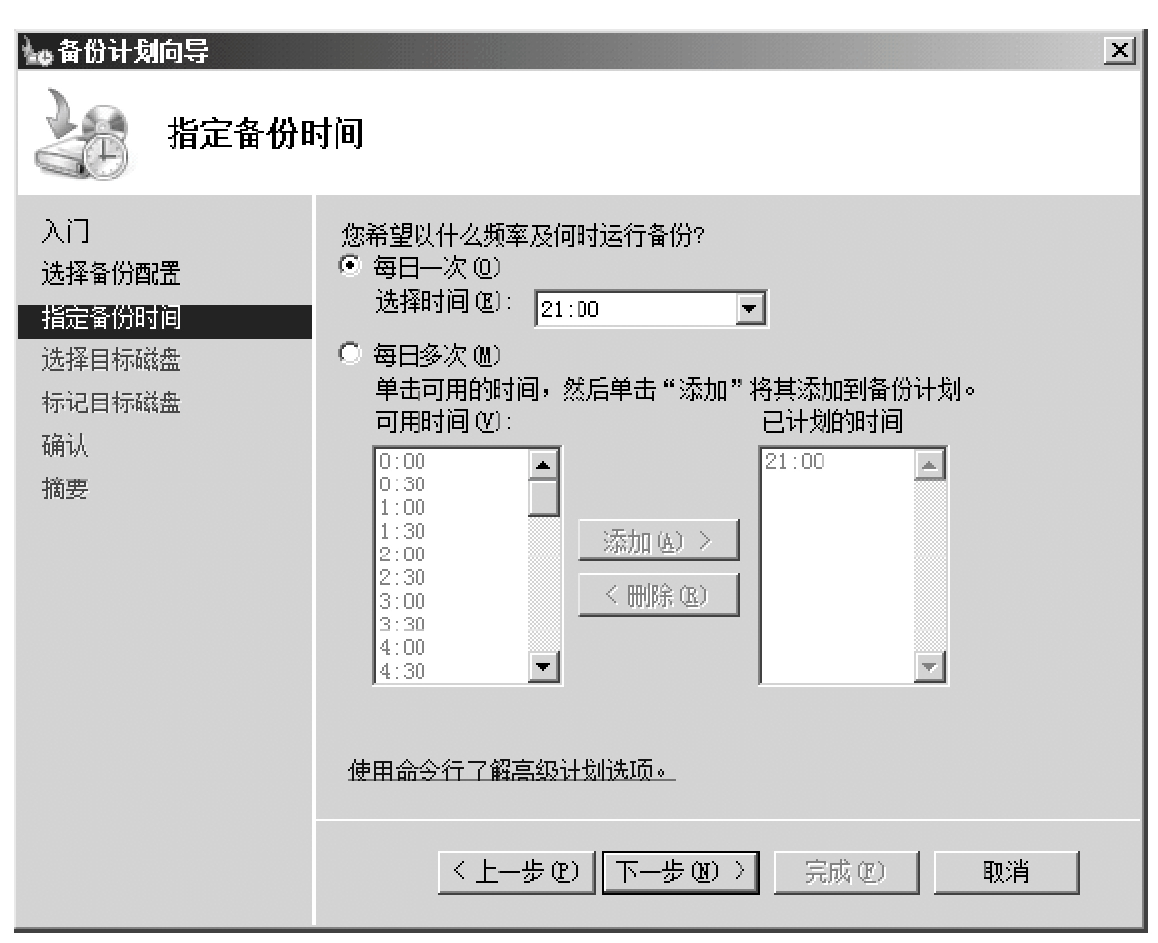


图 1-77　“指定备份时间”界面

(16) 设置备份频率完毕后，单击“下一步”按钮，进入“选择目标磁盘”界面，如图 1-78 所示。如果该界面中没有显示任何可用的磁盘，单击“显示所有可用磁盘”按钮，在弹出的对话框中选择作为备份的目标磁盘。

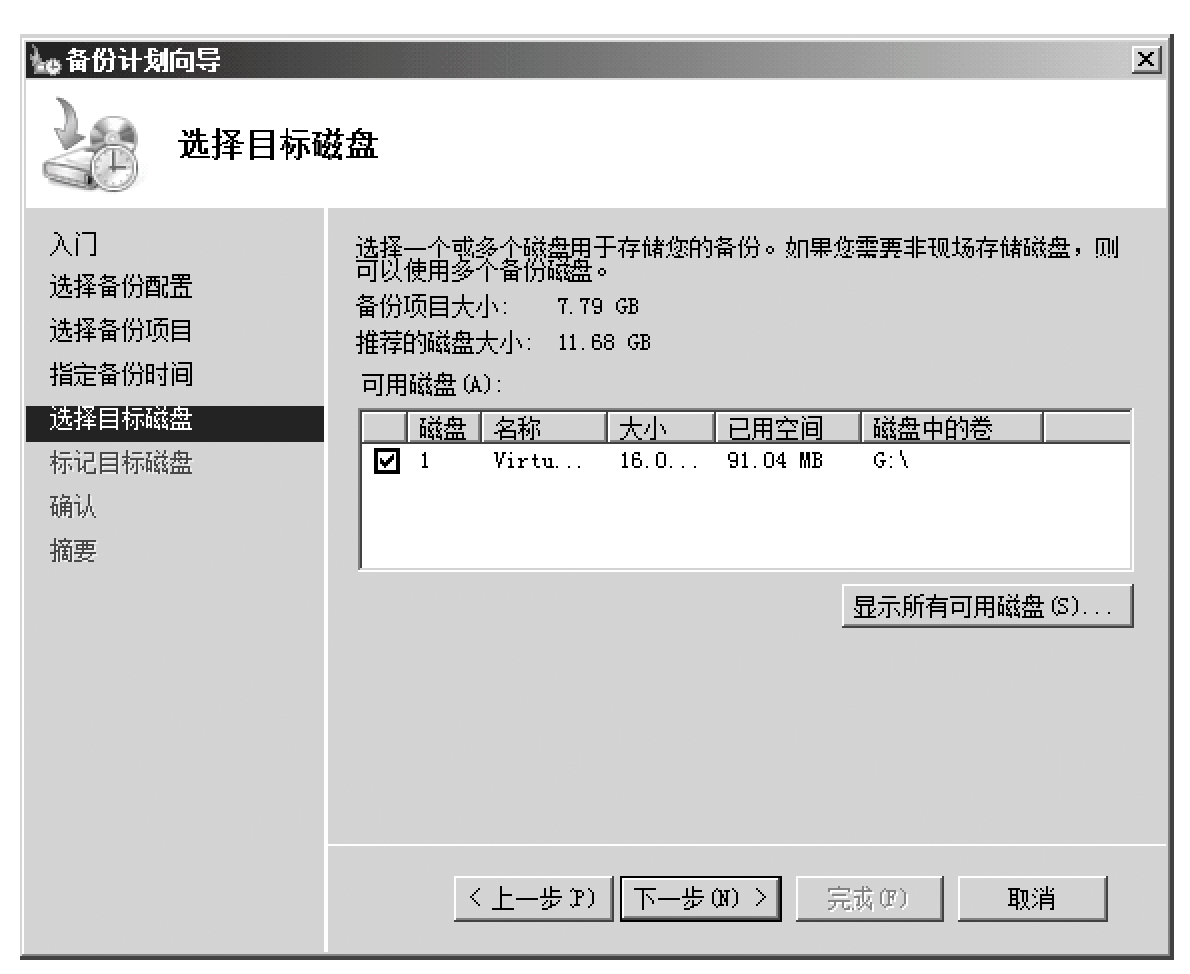


图 1-78　“选择目标磁盘”界面

(17) 选好磁盘后，单击“下一步”按钮，会弹出一个对话框提示要将该磁盘格式化，单击“是”按钮，进入“标记目标磁盘”界面，如图 1-79 所示。

(18) 单击“下一步”按钮，进入“确认”界面，单击“完成”按钮，开始格式化目标磁盘，等待几分钟后完成配置。

(19) 备份计划完成后，计算机将自动根据计划和备份模式设置对系统进行备份。

(20) 如果计算机出现故障，可以通过恢复备份将系统还原到正确的状态。在“Windows Server Backup”管理器中选择“恢复”选项，打开恢复向导，如图 1-80 所示。



图 1-79　“标记目标磁盘”界面

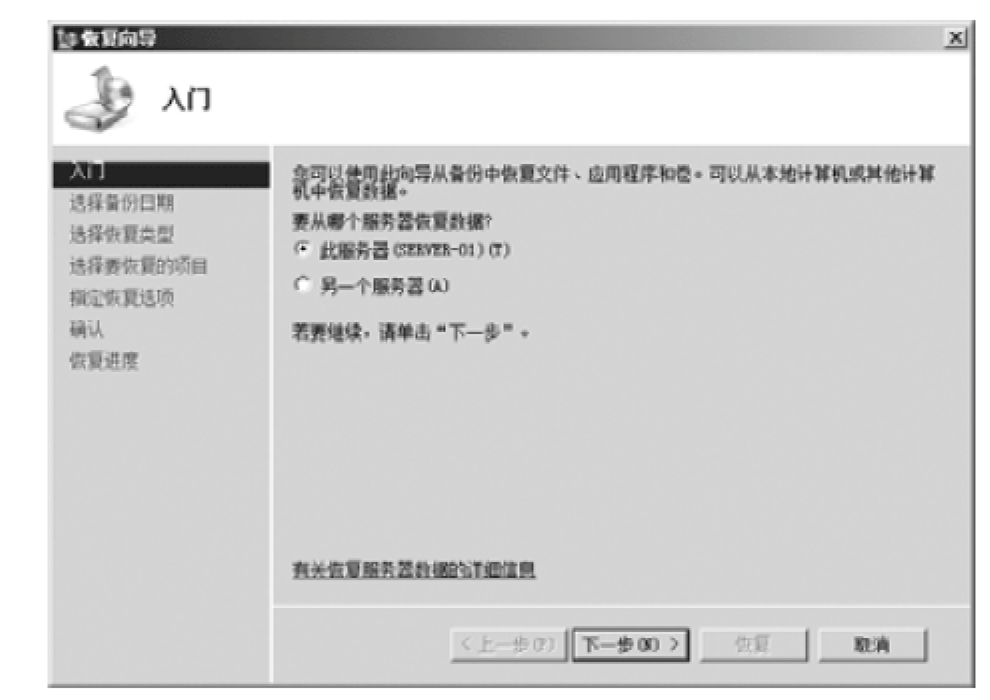


图 1-80　恢复向导欢迎界面

(21) 在该界面中选择为哪个服务器恢复备份，此处选择“此服务器”，即恢复本机的备份。选择完毕后，单击“下一步”按钮，进入“选择备份日期”界面，如图 1-81 所示。



图 1-81　“选择备份日期”界面

(22) 该界面中以日期标明备份，凡是做过备份的日期均以蓝底白字显示。如果一天中有多次备份，则以备份时间加以区分。选择要恢复的备份，单击“下一步”按钮，进入“选择恢复类型”界面，如图 1-82 所示。



图 1-82　“选择恢复类型”界面

(23) 在本界面中选择需要恢复的内容，如果选中“文件和文件夹”单选按钮，可以指

定恢复某些文件和文件夹；如果选中“应用程序”单选按钮，可以恢复一些应用程序；如果选中“卷”单选按钮，可以将整个卷的内容进行恢复。此处选中“卷”单选按钮，单击“下一步”按钮，进入“选择卷”界面，如图 1-83 所示。

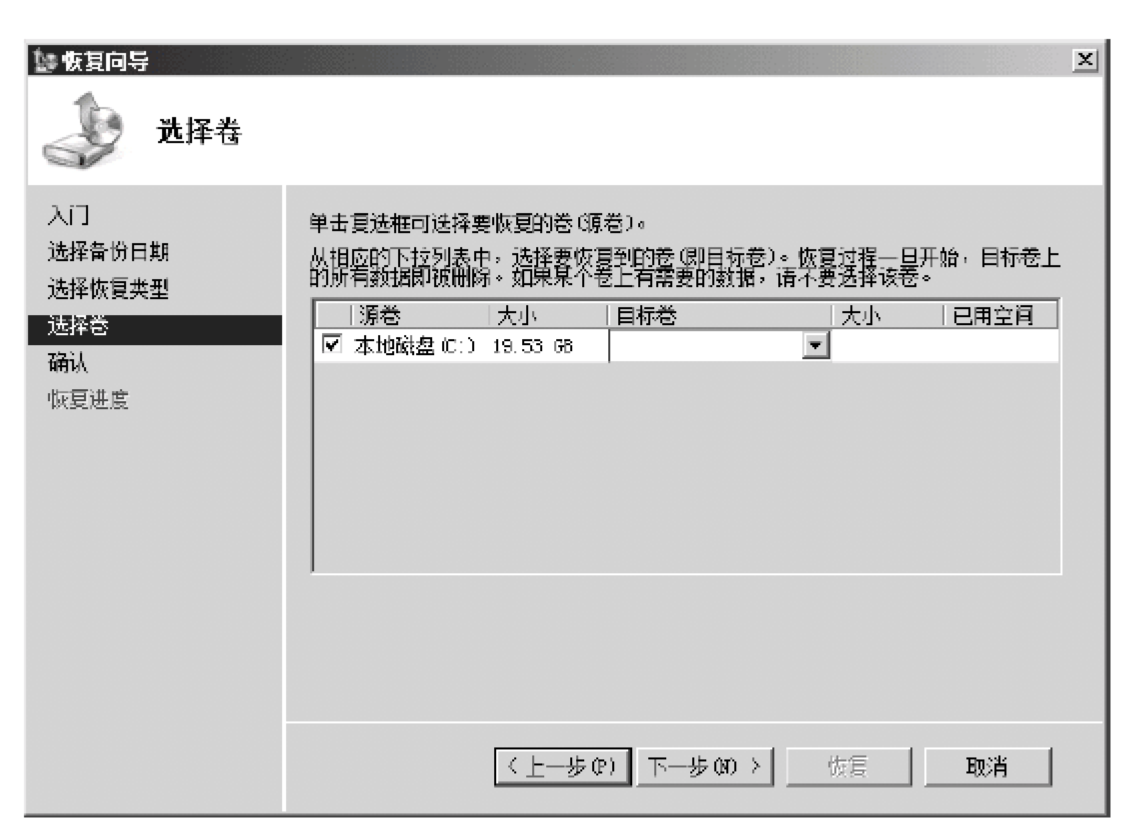


图 1-83　“选择卷”界面

(24) 选中要恢复的卷，单击“下一步”按钮进入确认界面，单击其中的“恢复”按钮，等待几分钟即可恢复完毕。

1.7　本章小结

通过本章学习，读者可以掌握选择正确的 Windows Server 2008 版本的标准，安装系统的方法和流程，并能对安装好的系统做简单的设置，为以后的使用做好铺垫。本章主要包括以下内容：

(1) Windows Server 2008 的版本和新特性：本节介绍了 Windows Server 2008 针对不同的应用市场、硬件配置和处理器类型所对应的不同版本，它们具有多种新特性，用户可以根据自己的需要选择不同的功能和版本，以便在有限的成本中最大限度地满足自身需求。

(2) Windows Server 2008 的安装：本节介绍了 Windows Server 2008 的多种安装方式，其中最主要的是全新安装和升级安装，有特殊需要的可以采用 Server Core 安装模式，用户可以根据自身条件选择合适的安装方式。

(3) Windows Server 2008 的基本配置：本节介绍了配置 Windows Server 2008 的桌面、计算机名、IP 地址、防火墙和连接网络的方法。

(4) Windows Server 2008 的管理：本节介绍了在 Windows Server 2008 中添加和删除角色的方法，使用控制台的方法，用户和用户组的概念和使用方法。

(5) Windows Server 2008 的初步使用：本节介绍了 Windows Server 2008 的基本使用方法，包括开机、关机、注销等常用操作。

(6) Windows Server 2008 启动故障排除：本节介绍了 Windows Server 2008 在出现故障

时可以使用的简单处理方法，以及如何为服务器创建备份和使用备份。

1.8　思考与练习

【思考题】

1. Windows Server 2008 的 Server Core 模式与普通的图形界面相比有何优势？为什么？

2. 如果用户的服务器硬件和操作系统均支持虚拟化技术，这项技术相比以往传统计算机系统，能够让用户在 Windows Server 2008 的网络管理中做出哪些调整？

3. 假设有一台服务器，已经安装了 Windows Server 2003 操作系统，但是漏洞百出，现在需将其升级至 Windows Server 2008，采取全新安装还是升级安装合适？为什么？

【练习题】

1. Windows Server 2008 有哪些版本？各有什么特点？
2. Windows Server 2008 有哪些安装方式，分别适用于什么情况？
3. 在 Windows Server 2008 中，如何安装服务器的角色？
4. 在 Windows Server 2008 中，如何创建和删除帐户？
5. Windows Server 2008 的启动高级选项有哪些？
6. Windows Server 2008 有哪几种备份模式？

第2章　文件服务

【本章导读】

文件服务是 Windows Server 2008 所提供的基本服务之一。文件服务提供了有助于管理存储、启用文件复制、管理共享文件夹、确保快速搜索文件等功能的相关技术；通过对共享文件夹的管理能够确保用户可以合适的身份、从合适的位置、在合适的权限控制下访问这些文件；通过分布式文件系统将分散的文件共享集成到单独的逻辑命名空间中进行管理，并使跨局域网或广域网网络连接的多台服务器上的文件夹能够实现同步。

2.1　文件服务与资源共享

2.1.1　安装文件服务器

文件服务功能是通过在 Windows Server 2008 中安装文件服务器实现的。安装文件服务器的步骤如下：

(1) 在“服务器管理器”中的“角色”对象上右击，在弹出的快捷菜单中选择“添加角色”命令，启动“添加角色向导”。

(2) 在“添加角色向导”对话框的“选择服务器角色”界面中，系统会列出 Windows Server 2008 系统所支持的所有角色类型，如图 2-1 所示，选中其中的“文件服务”选项，然后单击“下一步”按钮。



图 2-1　添加“文件服务”角色

(3) 随后出现的是文件服务的简要说明信息及安装文件服务的注意事项，并给出了文

件服务相关概念的帮助信息链接，如图 2-2 所示。

(4) 接下来在“添加角色向导”对话框的“选择角色服务”界面中选择需要为“文件服务”安装的“角色服务”种类，如图 2-3 所示，在此可根据需要进行选择。



图 2-2　“文件服务”设置界面

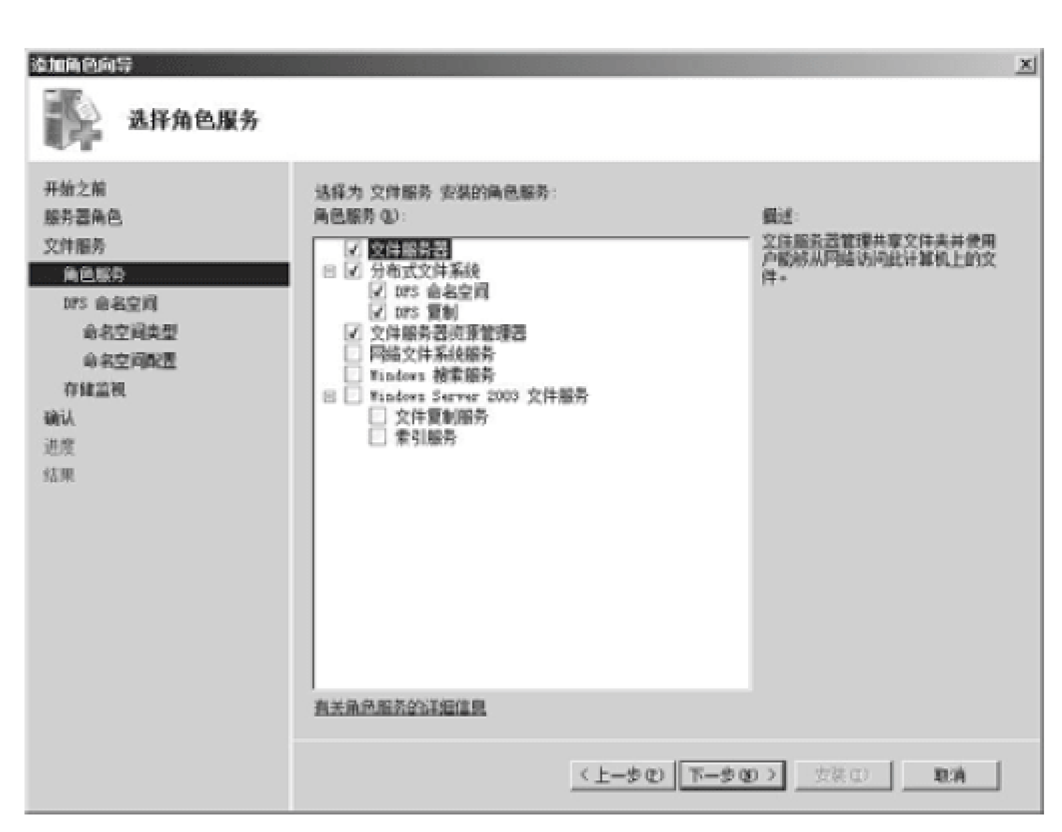


图 2-3　“选择角色服务”界面

- “文件服务器”用于管理共享文件夹并确保用户能够通过网络进行文件访问。这是“文件服务”的基本内容。
- “分布式文件系统”(Distributed File System，DFS)能够为 DFS 命名空间和 DFS 复制提供工具和服务。如选择此项，则“添加角色向导”会在后续步骤中提示用户进行 DFS 命名空间的相关设置。
- “文件服务器资源管理器”用于生成存储报告、配置配额，并定义文件屏蔽策略。如选择此项，则“添加角色向导”会在后续步骤中提示用户设置存储监视的对象和选项。
- “网络文件系统服务”提供针对 UNIX 客户端计算机的连通性并授予文件访问的权限。
- “Windows 搜索服务”能够对文件建立索引，以便为客户端连接共享文件提供更快

的搜索速度。如选择此项，则“添加角色向导”会在后续步骤中提示用户对用于承载共享文件夹的本地磁盘创建索引。需要注意的是，不能在同一台计算机上安装“Windows 搜索服务”和“索引服务”。因为这两种索引解决方案在主动对卷和文件夹编制索引时会消耗系统资源，同时运行这两种解决方案可能会严重影响系统性能。

- “Windows Server 2003 文件服务”能够提供与 Windows Server 2003 兼容的服务，包括文件复制服务和索引服务。

(5) 根据用户在前一步骤中所选择的“角色服务”种类，向导会相应地引导用户进行相关的设置。完成设置后，向导会跳转至“确认安装选择”界面，如图 2-4 所示，显示了前面步骤中所选择的“角色服务”类型和相关的参数设置情况，以便用户在正式安装前作最后的审核。需要注意的是，如果用户选择了“DFS 复制服务”，则必须保证该服务器已经加入到域中，否则就会出现图 2-4 中所示的警告信息提示。

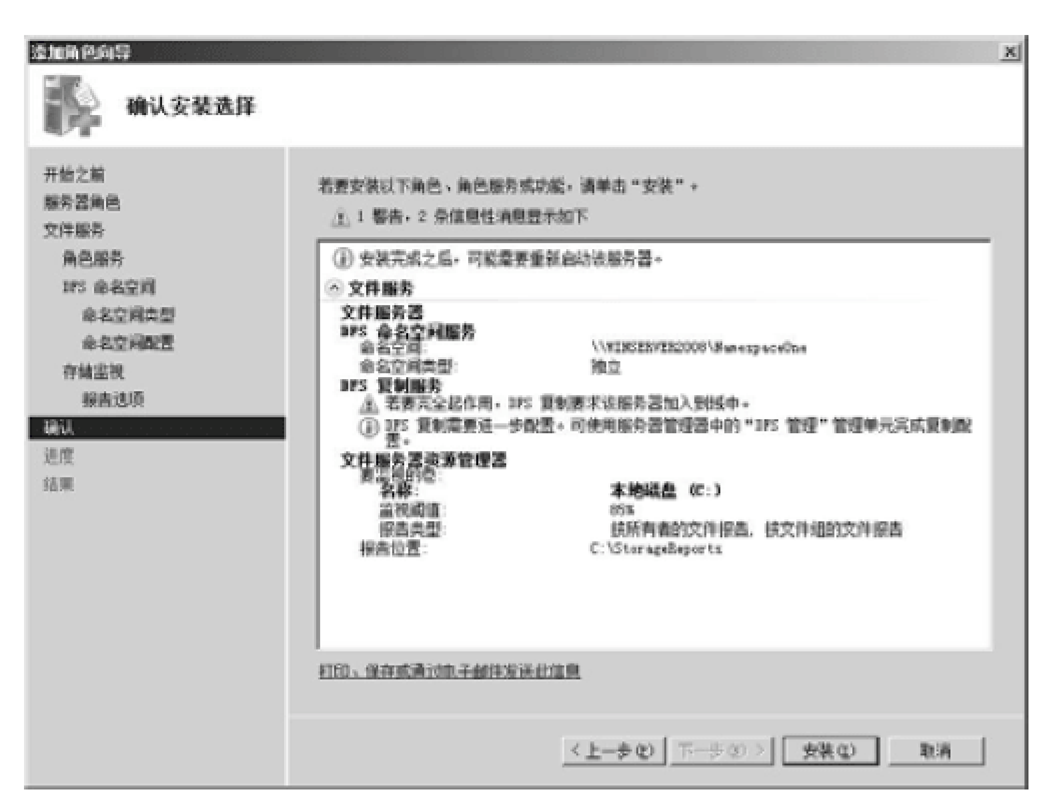


图 2-4　“确认安装选择”界面

(6) 单击“安装”按钮，开始安装文件服务器。安装完成后，会显示如图 2-5 所示的“安装结果”界面，并在列表中显示安装结果及检测到的问题。



图 2-5　“安装结果”界面

(7) 单击“关闭”按钮，完成“添加角色向导”的整个过程，返回到“服务器管理器”窗口。此时可以看到“服务器管理器”窗口中的提示信息表明文件服务器已经安装完成并开始提供服务，如图 2-6 所示。注意：“文件服务”前的警告标志表明 DFS 复制服务无法连接到域控制器以访问配置信息，因此无法开始复制。此问题可以通过在安装 Active Directory 域服务和 DNS 服务器时进行相关的参数设置解决。



图 2-6　安装文件服务后的服务器管理器

2.1.2　设置资源共享

资源共享是计算机网络最重要的功能之一。网络中的许多重要资源常常需要让许多具有权限的用户通过网络进行共享访问，这样不但能够有效节约费用，而且还能大大提升日常工作效率。但是资源共享如果没有进行细致的规划和谨慎的管理，也往往会成为网络入侵的主要通道。为了提高安全性，如果要为某个用户提供文件共享，必须先针对文件夹设置共享，然后再为用户分配相应的访问权限。

在 Windows Server 2008 系统中设置资源共享可以通过服务器管理器实现，也可通过简单文件夹共享方式实现，下面分别进行介绍。

1. 通过服务器管理器实现

在文件服务器中设置资源共享打开“服务器管理器”，依次展开“角色”和“文件服务”，选择“文件服务”中的“共享和存储管理”，此时窗口中部就会列出当前系统中所共享的文件夹列表，如图 2-7 所示。



图 2-7　服务器管理器中的共享和存储管理

单击窗口右部“操作”区域的“设置共享”链接，弹出如图 2-8 所示的“设置共享文件夹向导”对话框。

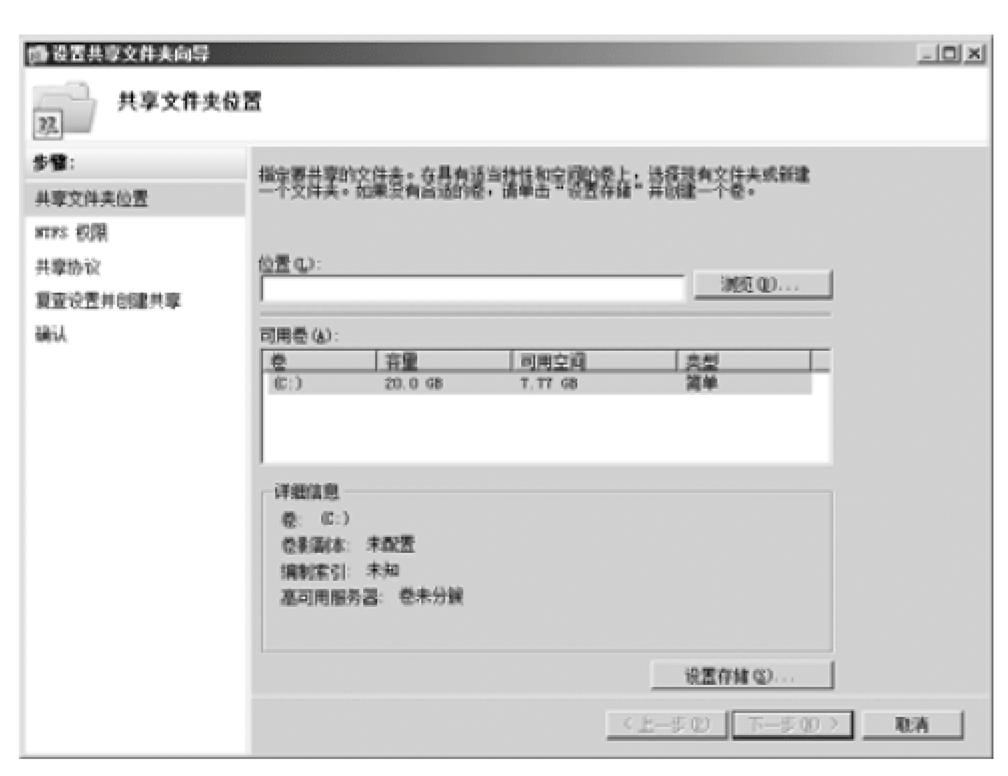


图 2-8　“设置共享文件夹向导”对话框

在“设置共享文件夹向导”对话框的“共享文件夹位置”界面，通过“浏览”按钮或直接在文本框中输入文件夹地址来选定要进行共享设置的文件夹，然后单击“下一步”按钮。

在“NTFS 权限”界面中根据需要选择是否要更改文件夹的 NTFS 权限。指定 NTFS 权限可以控制具体用户和用户组在本地访问文件夹(NTFS 权限的设定请参阅下节内容)，网络中的用户访问此共享文件夹时，系统会以登录用户的权限来控制对共享文件夹的访问。

在接下来的“共享协议”界面中可以逐一选择可供用户访问共享文件夹的协议。有 SMB 和 NFS(必须在服务器上安装网络文件系统服务方可选中该项)两种方式可供选择。

如选择通过“SMB”共享协议方式共享文件夹，则在接下来的“SMB 设置”界面中还需要给共享文件夹添加相应的描述，并进行相关的高级设置，如指定能同时访问共享文件夹的用户数量限制等，如图 2-9 所示。



图 2-9　设置共享文件夹向导-SMB 设置

接下来还需要在“SMB 权限”界面中为基于 SMB 的共享文件夹访问指定共享权限，如图 2-10 所示。可以通过选择某个单选按钮选项来为所有用户或用户组指定统一的访问权限，也可以在选中“用户和组具有自定义共享权限”单选按钮后单击“权限”按钮，针对

特定的用户或用户组进行单独的访问权限设置。

在下一步骤中可以将共享文件夹发布到现有的 DFS 命名空间中，并指定该文件夹在命名空间中的新名称如图 2-11 所示。

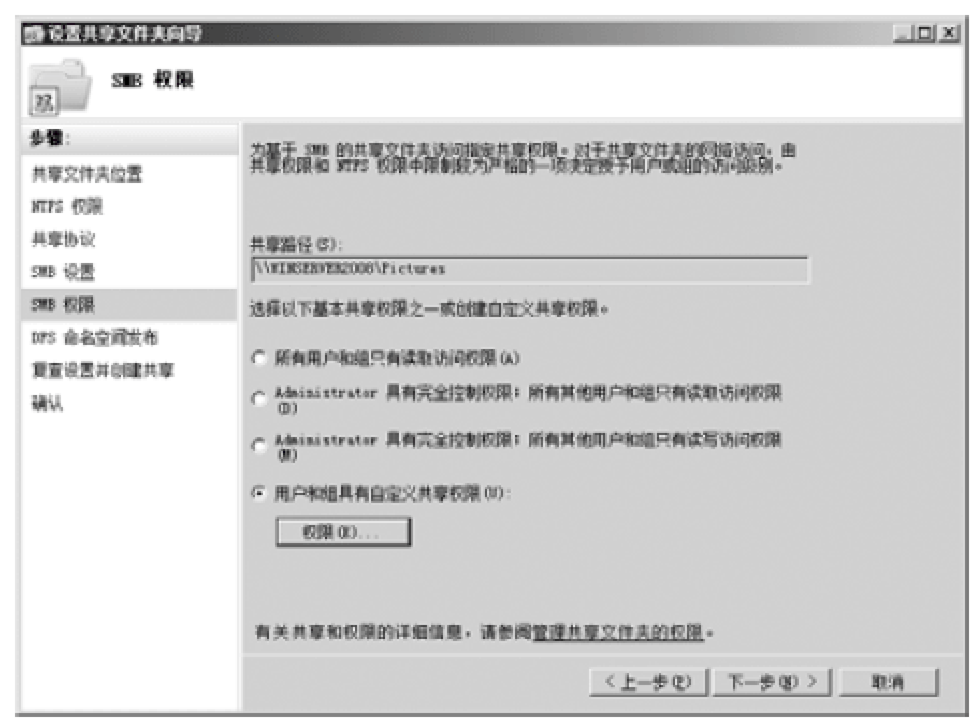


图 2-10　设置共享文件夹向导-SMB 权限



图 2-11　设置共享文件夹向导-DFS 命名空间发布

在“复查设置并创建共享”界面中可以集中审查在前述各步骤中所作的设置。如有需要修改的地方，可以单击对话框左侧的步骤链接返回到相应的步骤进行修改；如果没有问题，则可单击“创建”按钮开始共享文件夹的设置，完成后“设置共享文件夹向导”对话框会自动跳转到“确认”界面，提示用户相关的文件夹共享设置已经完成，如图 2-12 所示，此时单击“关闭”按钮即可完成共享文件夹设置过程。在“共享和存储管理”窗口中部可立刻看到刚才设置的共享文件夹已经被添加到共享文件夹列表中。

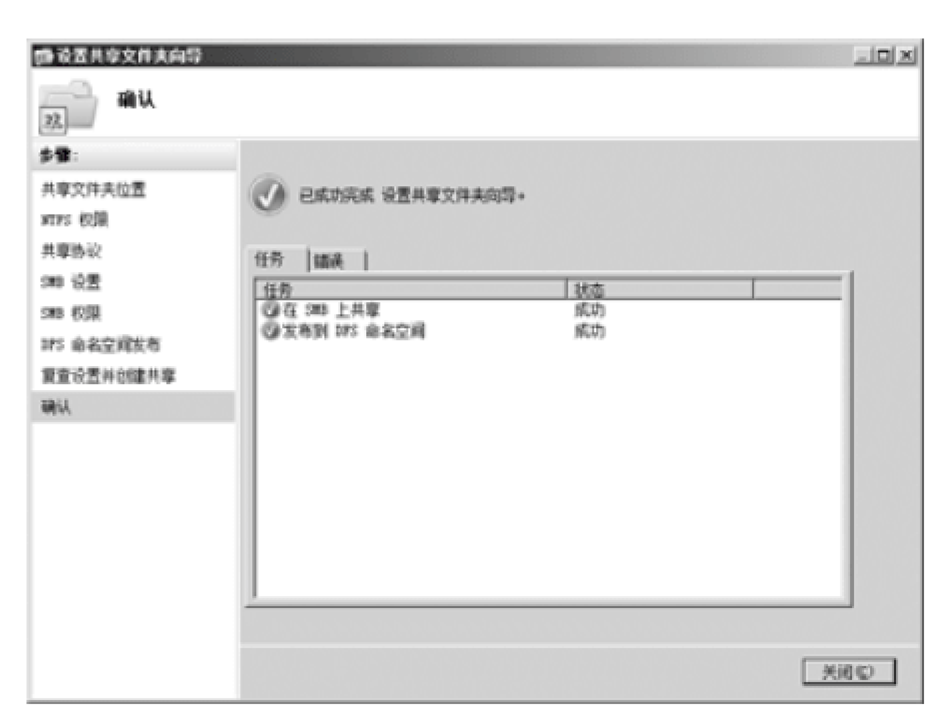


图 2-12　设置共享文件夹向导-确认

2. 通过简单文件夹共享方式实现

在需要进行共享的文件夹上右击，在弹出的快捷菜单中选择“共享”菜单项(或单击文件夹所在的窗口上方的“共享”按钮)，弹出“文件共享”对话框，如图 2-13 所示。

在“文件共享”对话框中输入想要共享的用户或用户组名称，然后单击“添加”按钮(如果不清楚用户名，也可以通过下拉框中的“查找”项进行查找)，新的共享用户或用户组就会添加到对话框下部的用户列表中，如图 2-14 所示。在此列表中还可以进一步确定用户的共享权限级别。Windows Server 2008 提供给共享用户或用户组的权限级别共有以下 3 种。

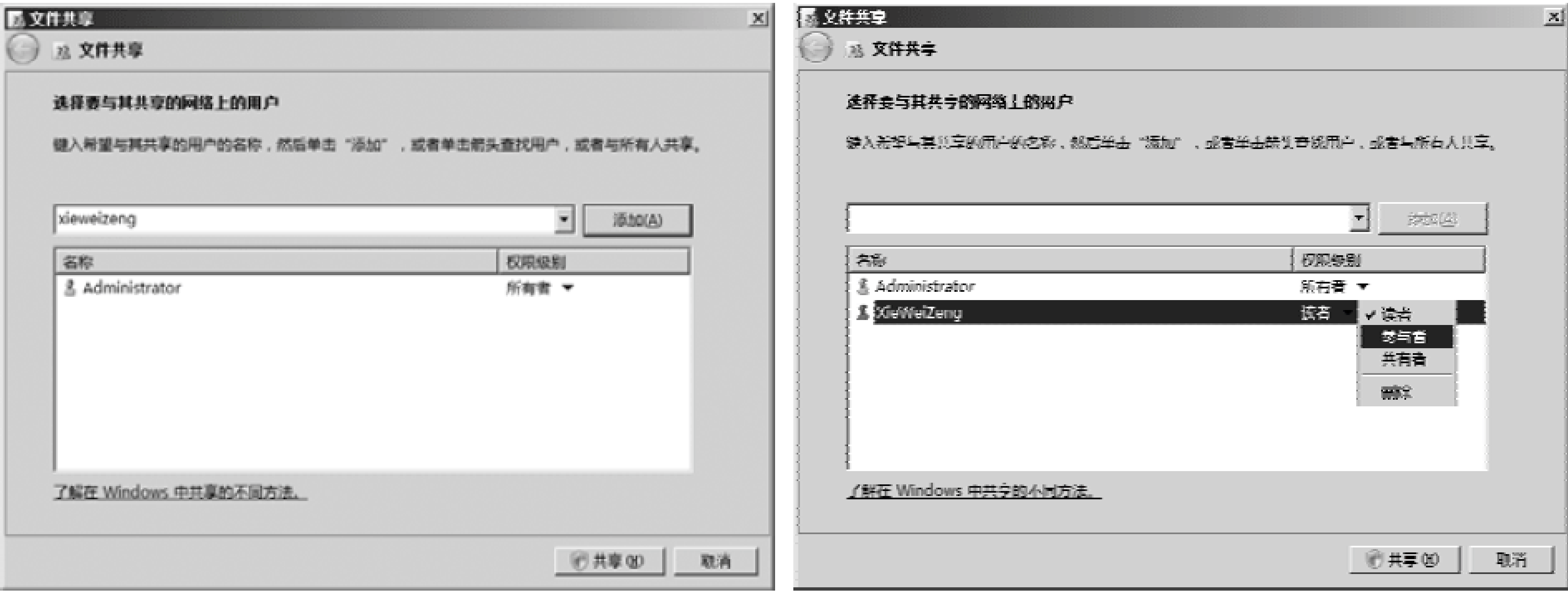


图 2-13　“文件共享”对话框　　　　图 2-14　选择共享用户

- 读者：限制共享用户或组只能查看共享文件夹中的文件。
- 参与者：允许共享用户或组查看所有文件、添加文件，以及更改或删除其所添加的文件。
- 共有者：允许共享用户或组查看、更改、添加和删除共享文件夹中的文件。

需要注意的是，如果共享的是文件而不是文件夹，则不能选择将权限级别设置为“参与者”。

添加好共享用户或用户组并指定相应的权限级别以后，单击“共享”按钮，经过短暂的时间后，就会看到文件夹已共享的提示信息，如图 2-15 所示，网络中的授权用户就可以通过提示信息中的地址访问这个共享资源了。

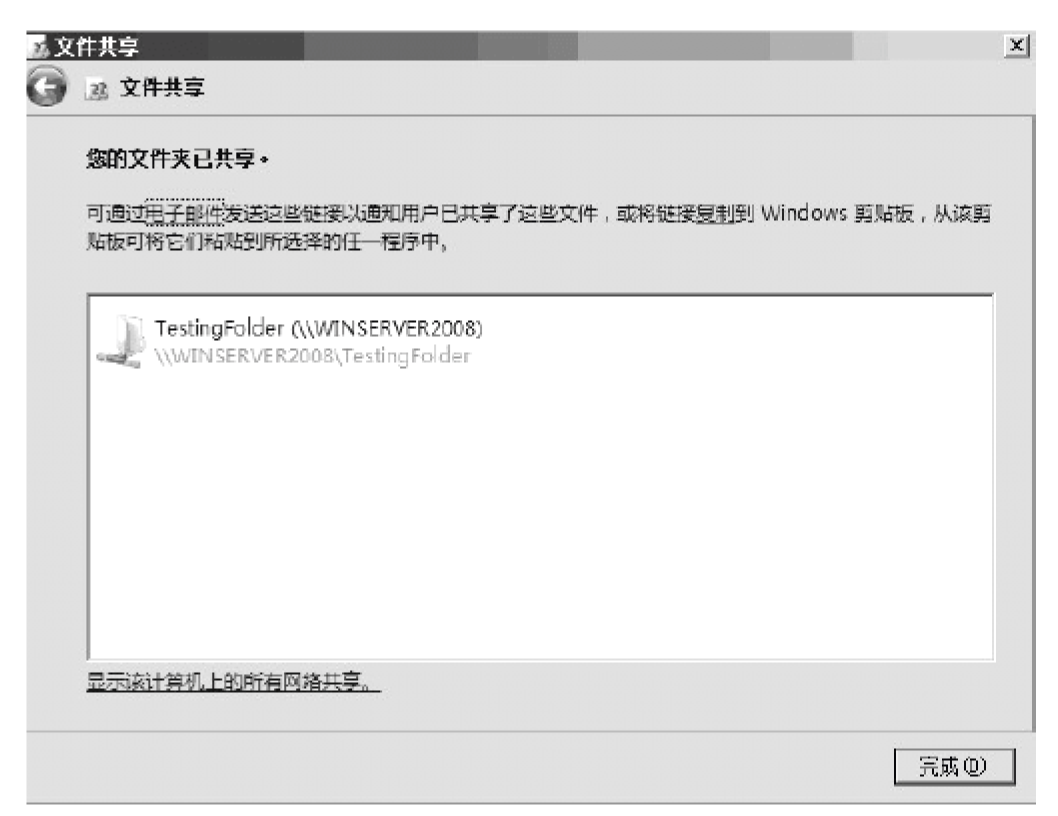


图 2-15　文件共享提示信息

2.1.3　访问网络共享资源

资源共享的目的就是为了使用户能够方便地通过网络访问文件资源。用户可通过多种方式访问网络共享资源。主要有以下 4 种。

(1) 通过网上邻居访问

位于同一个工作组或域的计算机上的共享资源都会显示在“网上邻居”当中，如果用户拥有相应的访问权限，即可实现对该共享资源(文件或打印机等)的访问，如图 2-16 所示。



图 2-16　通过“网上邻居”访问共享资源

(2) 通过搜索计算机访问

如果网上邻居中没有显示出包含网络共享资源的服务器，则可以通过“搜索”功能进行查找。打开搜索对话框后，在“搜索其他项”位置选中“计算机”，在“计算机名”文本框中输入要搜索的服务器的名称或 IP 地址，然后单击“立即搜索”按钮，系统即可在当前网络中搜索指定的计算机并将搜索结果显示在对话框右侧，如图 2-17 所示。用户可以通过单击搜索结果对服务器进行连接进而访问服务器上的共享资源。当然这也要求访问者有正确的用户身份和适当的访问权限。



图 2-17　搜索计算机访问共享资源

(3) 通过映射网络驱动器访问

前述方式都需要用户记住共享资源所在的服务器名称和共享文件夹的名字，如果需要经常访问共享资源，这样就会比较麻烦，映射网络驱动器刚好能解决这个问题。它能够使用户对网络共享资源的访问就像对本地驱动器的访问一样方便。

在“我的电脑”窗口的“工具”菜单下选择“映射网络驱动器”命令，就会弹出如图 2-18 所示的“映射网络驱动器”对话框。在“驱动器”下拉列表中选择一个当前未被使用的英文字母作为网络驱动器的盘符，在“文件夹”文本框中以“\\服务器名称\共享文件夹

名称”的格式输入服务器名称和共享文件夹名称。如果当前的用户身份没有合适的访问权限，则需要单击“其他用户名”链接，在随后弹出的“连接身份”对话框中输入能够访问共享资源的用户名以及密码，如图 2-19 所示。设置完成后，单击“确定”按钮，系统即可将网络共享资源映射为一个指定的驱动器，与 C:、D:等本地驱动器一样放在“我的电脑”窗口中，如图 2-20 所示。

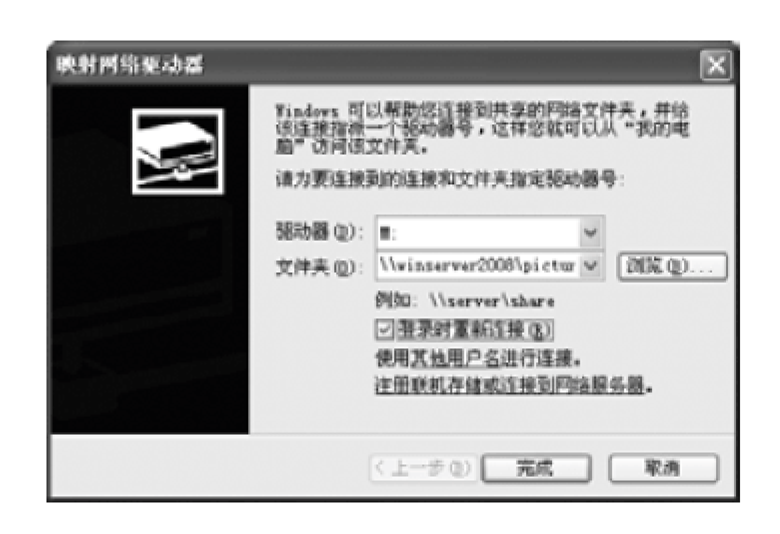


图 2-18　“映射网络驱动器”对话框



图 2-19　“连接身份”对话框



图 2-20　映射后的网络驱动器

(4) 通过地址栏访问

还有一种更为便捷的访问方法，就是直接通过“我的电脑”或“Windows 资源管理器”(或任何一个附带地址栏的)窗口，在地址栏(如果地址栏没有显示出来，可以通过“查看”→“工具栏”→“地址栏”菜单项使其显示)中直接以“\\服务器名称\共享文件夹名称”的格式输入服务器名称和共享文件夹名称，就可以访问共享资源了，如图 2-21 所示。当然前提也是用户须具备访问服务器和共享文件夹的有效权限。



图 2-21　通过地址栏访问资源

共享资源的访问必须经过严格的身份认证和权限审核，除此以外，服务器管理员还可

以随时监控网络用户对共享资源的访问情况，包括当前正在访问共享资源的用户身份、主机 IP 地址、操作系统类型、打开文件数量、连接时间及空闲时间等信息，如图 2-22 所示，如有必要，管理员还可以随时中断特定用户对共享资源的访问，中止其连接。

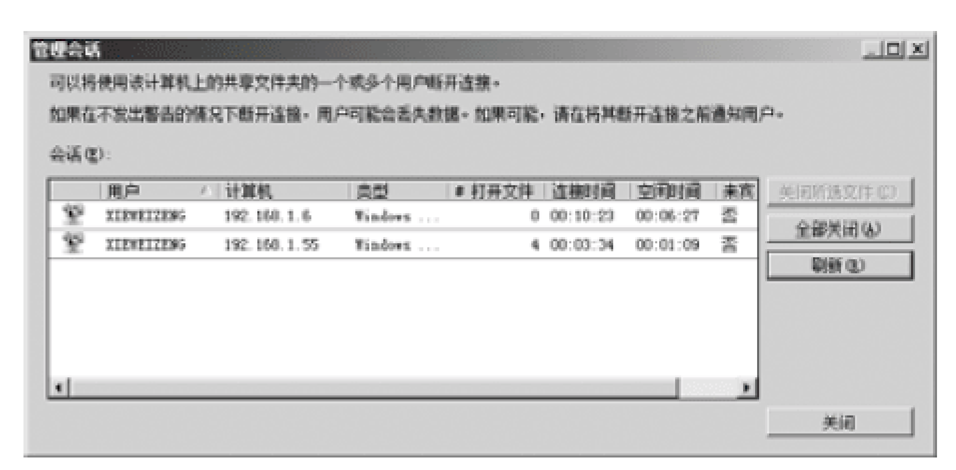


图 2-22　“管理会话”对话框

2.2　NTFS 权限

2.2.1　NTFS 权限概述

NTFS 全称为 New Technology File System，是微软公司从 Windows NT 3.1 起的各版本 Windows 系列操作系统，包括 Windows Server 2008、Windows Vista 和 Windows 7 等所采用的标准文件系统。NTFS 拥有许多先进的技术特性，并且使用了高级数据结构，支持数据压缩和磁盘限额，可以改善磁盘性能、可靠性和空间利用率，并通过加密文件系统(EFS)提供对 NTFS 卷上任意文件和文件夹的用户透明的强保护。

NTFS 权限是 NTFS 提供的用于文件系统安全的重要特性。利用 NTFS 权限，管理员可以完全控制用户或用户组对每个文件和文件夹的访问。NTFS 权限只适用于采用 NTFS 文件系统的磁盘分区，而不能用于 FAT 或 FAT32 文件系统。要想访问 NTFS 磁盘分区上的文件或文件夹，用户必须拥有相应的 NTFS 权限。对于 NTFS 磁盘分区上的每一个文件及文件夹，NTFS 都存储一个访问控制列表(Access Control Lists，ACL)。访问控制列表中包含了被授权访问该文件或文件夹的所有用户、用户组及计算机的信息，还包含了其被授予的访问类型。

NTFS 文件权限有以下 5 种。

- 读取：允许用户读取文件的数据，查看文件的所有者、属性和权限信息。
- 写入：允许用户改写文件内容、更改文件属性及查看文件的所有者和权限。
- 读取和执行：使用户拥有“读取”的所有权限，并可以运行应用程序。
- 修改：允许用户拥有“读取”、“写入”和“读取和运行”的所有权限，并可以修改、删除文件。
- 完全控制：允许用户拥有对该文件的完全控制，即前述的所有权限，并可以更改现有权限设置和取得所有权的权限。

NTFS 文件夹权限有以下 6 种。

- 读取：允许用户查看文件夹内的文件和子文件夹，查看文件夹属性、权限和所有者信息。
- 写入：允许用户在文件夹内创建新文件和子文件夹，改变文件夹属性，查看文件夹的权限和所有者。
- 列出文件夹目录：使用户拥有“读取”的所有权限，同时还具有“遍历子文件夹”的权限，以便能够进入子文件夹并查看其内容。
- 读取和执行：使用户拥有“读取”和“列出文件夹目录”的所有权限，不过在继承方面有所不同：“列出文件夹目录”权限仅由文件夹继承，“读取和执行”权限由文件和文件夹同时继承。
- 修改：使用户拥有“写入”和“读取和执行”的所有权限，并可以删除文件夹。
- 完全控制：允许用户拥有对该文件夹的所有权限，并可以更改现有权限设置和取得所有权的权限。

2.2.2　NTFS 权限的设置

在 NTFS 磁盘分区中，系统会自动为所有文件和文件夹设置默认的权限值，文件夹的权限又会被其子文件夹和文件所继承。一般的用户是不能修改文件或文件夹的 NTFS 权限的，只有 Administrators 用户组的成员、文件或文件夹的所有者、具有对该文件或文件夹“完全控制”权限的用户才可以修改或重新指定 NTFS 权限。

尽管可以分别对文件和文件夹设置 NTFS 权限，但为了管理方便，通常不直接为文件设置权限，而是将需要设置为相同权限的文件放置到同一个文件夹中，然后对该文件夹设置权限。

1. 设置 NTFS 文件夹的权限：

在欲设置 NTFS 文件夹权限的文件夹上右击，在弹出的快捷菜单上选择“属性”命令，在弹出的“属性”对话框中选择“安全”选项卡，如图 2-23 所示。“安全”选项卡的上部显示了对当前文件夹拥有权限的用户和用户组列表，在列表中选中某个用户或用户组后选项卡的下部就会显示该用户或用户组实际拥有的权限类型。

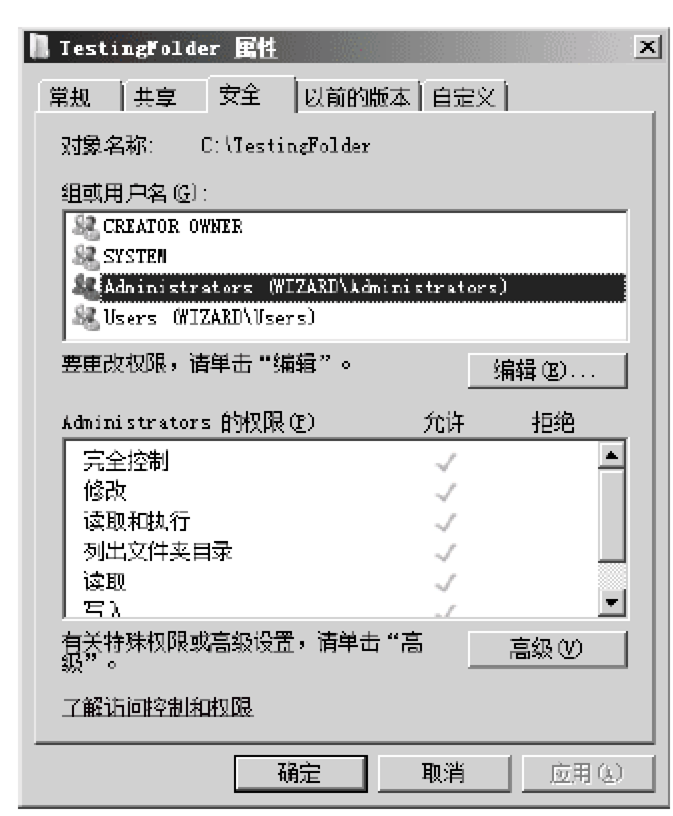


图 2-23　文件夹属性对话框

如果需要修改该文件夹的 NTFS 权限设置，单击“编辑”按钮，将弹出如图 2-24 所示的文件夹“权限”对话框。此对话框的上部依然是对当前文件夹拥有权限的用户和用户组列表，下部显示了当前选中的用户或用户组对文件夹拥有的 NTFS 权限。要使用户或用户组拥有某项 NTFS 权限，只需选中权限对应行的“允许”复选框即可，要想取消用户或用户组已拥有的某项 NTFS 权限，

只需取消相应权限对应行的“允许”复选框即可。

如果需要给其他用户或用户组指派权限，或删除某用户或用户组对该文件夹所拥有的权限，在图 2-24 所示的“权限”对话框中单击相应的“添加”或“删除”按钮即可。在添加用户时，需要先选择要添加的用户或用户组，如图 2-25 所示，选定以后会返回到“权限”对话框，此时添加的用户或用户组会显示在对话框上部的列表中，并处于选中状态，如图 2-26 所示。系统会自动为新添加的用户或用户组赋予“读取和执行”、“列出文件夹目录”和“读取”3 种基本权限，用户可以根据需要进行调整。如果需要给新添加的用户或用户组赋予某种权限，只需在相应权限位置选中“允许”复选框即可；反之则不必选中“允许”复选框。

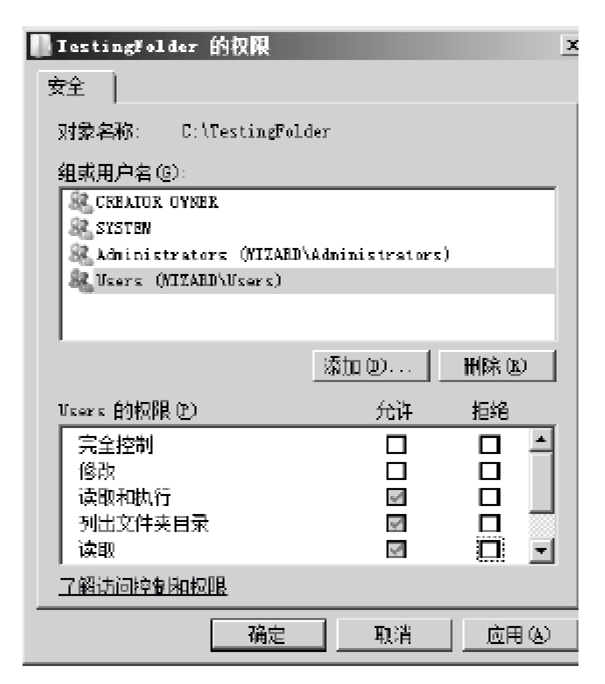


图 2-24　文件夹权限对话框



图 2-25　“选择用户、计算机或组”对话框



图 2-26　新用户的权限设置

2. 设置 NTFS 文件权限

文件与文件夹的权限设置非常相似，通过打开文件“属性”对话框，切换到“安全”选项卡，显示当前拥有权限的用户或用户组清单及其所拥有的权限类型如图 2-27 所示，单击“编辑”按钮，弹出“权限”对话框，如图 2-28 所示，进行用户或用户组的添加、删除，或对当前拥有权限的用户或用户组进行权限的调整。



图 2-27　文件属性对话框



图 2-28　文件权限设置对话框

设置权限是一项工作量大且复杂的工作，而权限继承可以让这项工作变得轻松。继承权限是从父对象(如文件夹)传播到子对象(如子文件夹)的权限。继承权限可以简化管理权限的任务，并确保给定容器中所有对象之间的权限一致。如果访问控制用户界面各个部分中的“允许”和“拒绝”权限复选框在查看对象的权限时显示为灰色，则说明该对象具有来自父对象的继承权限。通常情况下子对象所拥有的权限与父对象是一致的，但有时候也可能需要对特定的子对象设置不同的权限，此时可以在文件夹“属性”对话框中单击“高级”按钮，弹出如图 2-29 所示的“高级安全设置”对话框，在该对话框的“权限”选项卡中设置这些继承权限。有以下 3 种推荐方式可对继承权限进行更改：

- 取消选中“包括可从该对象的父项继承的权限”复选框，然后便可对权限进行更改或删除“权限”列表中的用户或组。但是，该对象将不再从其父对象继承权限。
- 对明确定义权限的父对象进行更改，然后子对象将继承这些权限。
- 编辑对象的权限项目，选择“允许”权限替代继承的“拒绝”权限，或选择“拒绝”权限替代继承的“允许”权限。这是因为直接选择的权限是显式权限(在复选框中以黑色表示)，而显式权限的优先级高于继承权限(在复选框中以灰色表示)。例如图 2-30 所示的情况，用户组 Users 从父对象那里继承得到了对文件夹 TestingFolder 的“读取属性”权限和“读取扩展属性”权限，要想取消这两个权限，就可以通过直接选中这两个权限的“拒绝”权限复选框来实现。

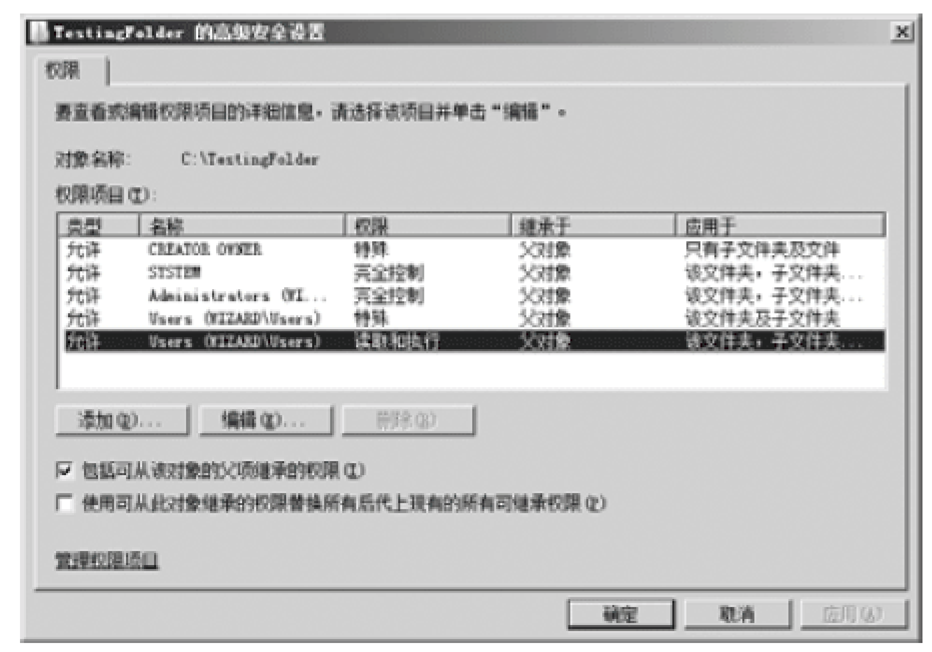


图 2-29　“高级安全设置”对话框

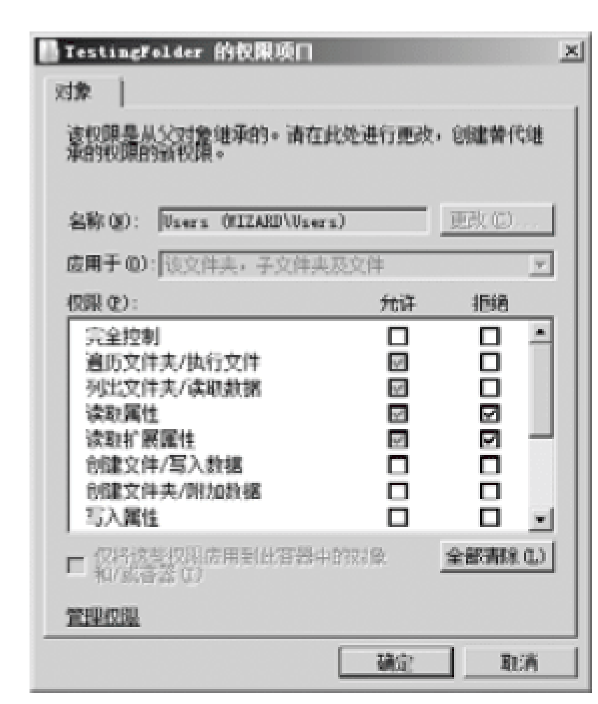


图 2-30　显式权限设置

2.2.3　共享权限与 NTFS 权限

访问文件服务器上的文件夹可通过两组权限条目来确定：文件夹上设置的共享权限和 NTFS 权限(也可在文件上设置)。共享权限经常用于管理具有 FAT32 文件系统的计算机，或其他不使用 NTFS 文件系统的计算机。但是当共享资源位于 NTFS 磁盘分区时，该共享资源的共享权限就会与 NTFS 权限进行组合，用于保护文件资源。共享权限提供资源共享的安全保证，NTFS 权限限制用户对文件夹的访问。

共享权限和 NTFS 权限是独立的，不能彼此更改。对于共享文件夹的最终访问权限是考虑共享权限和 NTFS 权限项后确定的，最终将应用更为严格的权限。

不论是在本地访问，还是通过网络访问该资源，NTFS 权限都发挥作用。NTFS 权限的应用与协议无关。相反，共享权限只适用于网络共享。共享权限将不限制已设置了共享权限的计算机上的任何本地用户或任何终端服务器用户访问。因此，共享权限不为多个用户使用的计算机上的用户，以及多个用户访问的终端服务器上的用户提供隐私。

如果要为共享文件夹设置 NTFS 权限，可以在共享文件夹的“属性”对话框中打开“安全”选项卡，然后对享有权限的用户或用户组及其所享有的 NTFS 权限进行设置。

共享文件夹权限与 NTFS 权限的区别在于：

- 共享文件夹权限仅适用于通过网络访问共享资源的用户，并不对直接登录到计算机的本地用户起作用；而 NTFS 权限无论是通过网络访问还是本地访问都会发挥作用。
- 共享文件夹权限只适用于文件夹，不适用于单独的文件。只能为整个共享文件夹设置共享权限，而不能针对该共享文件夹中的文件或子文件夹进行设置；而 NTFS 权限能够针对共享文件夹中包含的每个文件和子文件夹进行不同的设置。
- 在 FAT/FAT32 文件系统中，无法使用 NTFS 权限控制共享文件夹的访问，此时只能通过共享文件夹权限来保证网络资源被安全访问。

当共享文件夹权限与 NTFS 权限进行组合时，组合结果所产生的权限或者是组合的 NTFS 权限，或者是组合的共享文件夹权限，哪个范围更窄、限制更严，就用哪一个。

2.2.4　文件与文件夹的所有权

在 NTFS 磁盘分区中，每个文件或文件夹都有其“所有者”(Owner)。默认情况下，创建文件或文件夹的用户就是其所有者。所有者具备更改该文件或文件夹权限的能力。但有些情况下需要改变文件或文件夹的所有者身份，让另一个用户取得文件或文件夹的所有权。

通常只有系统管理员，即隶属于 Administrators 用户组的用户才拥有更改某个文件或文件夹所有权的能力，因为系统管理员对文件或文件夹具有“取得所有权”的权限。不过其他具备“取得文件或其他对象所有权”权限的用户或是对该文件或文件夹拥有“取得所有权”权限的用户，也能够改变所有权。具体操作过程如下：

(1) 选中要更改所有权的文件或文件夹，右击后选择快捷菜单中的“属性”命令，在弹出的“属性”对话框中单击打开“安全”选项卡，然后单击“高级”按钮，弹出“高级安全设置”对话框，单击打开“所有者”选项卡，如图 2-31 所示。此时即可查看文件或文件夹的当前所有者以及能够获得所有权的用户列表。



图 2-31　查看当前所有者

(2) 单击“编辑”按钮，即可打开如图 2-32 所示的更改所有者对话框，通过此对话框，可以将文件或文件夹的所有者变更为系统管理员或系统管理员组，也可以变更为其他某个指定的用户或用户组，这通过单击“其他用户或组”按钮实现。



图 2-32　更改所有者对话框

(3) 修改完成后，单击“确定”按钮保存修改结果。系统会自动显示如图 2-33 所示的信息，提示用户在查看或更改权限之前，需要关闭并重新打开文件或文件夹的属性对话框。

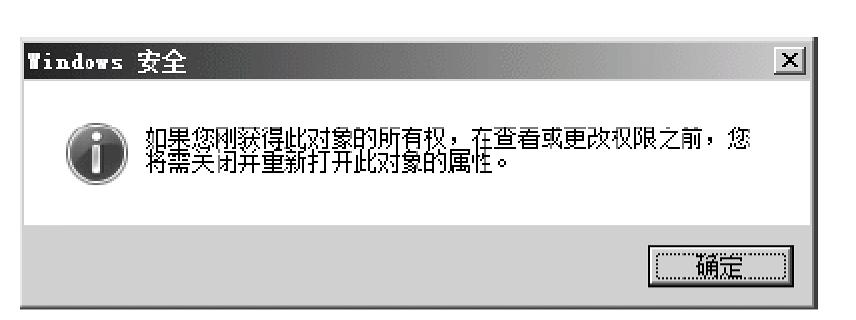


图 2-33　更改所有权提示信息

2.2.5　文件权限的变化

对于 NTFS 磁盘分区内的文件，当复制或移动到另一个文件夹后，其权限可能会发生如下变化：

(1) 当文件从一个文件夹复制到另一个文件夹时，无论这两个文件夹位于同一个 NTFS 磁盘分区还是不同的 NTFS 磁盘分区，都相当于创建了一个新的文件，因此新文件的权限将继承目标文件夹的权限。

(2) 当文件从一个文件夹移动到另一个文件夹时，如果是移动到同一个 NTFS 磁盘分区的文件夹中，则文件会仍然保持原来的权限；如果是移动到另一个 NTFS 磁盘分区，则文件会继承目的地的权限。

(3) 将文件移动或复制到目的地的用户将拥有该文件的所有权。

文件夹的移动或复制时权限的变化与文件是一样的。需要注意的是，在移动文件或文件夹时，无论移动到相同还是不相同的 NTFS 磁盘分区，用户都必须对来源文件或文件夹拥有“修改”权限，同时还必须对目的文件夹拥有“写入”权限。

由于 FAT/FAT32 文件系统不支持 NTFS 权限的设置，所以当文件从 NTFS 磁盘分区被

复制或移动到 FAT 或 FAT32 磁盘分区上时，其原有的权限设置都将被删除。

2.3　磁盘配额

磁盘配额就是管理员为用户所能使用的磁盘空间进行配额限制。设置磁盘配额后，管理员可以对每一个用户的磁盘使用情况进行跟踪和控制，可以通过监测标识出超过配额报警阈值和配额限制的用户，从而采取相应的措施。

磁盘配额是以文件所有权为基础的，只应用于 NTFS 卷，且不受卷的文件夹结构和卷在物理磁盘上的布局影响。它独立地监视用户对 NTFS 卷的使用情况，用户与用户之间对卷的使用不会相互影响。

磁盘配额管理功能的提供，使得管理员可以方便合理地为用户分配存储资源，可以限制指定帐户能够使用的磁盘空间，这样可以避免因某个用户的过度使用磁盘空间造成其他用户无法正常工作甚至影响系统运行，避免由于磁盘空间使用的失控可能造成的系统崩溃，提高了系统的安全性。

2.3.1　磁盘配额的功能

只有管理员或拥有管理员权限的用户才能启用磁盘配额功能，并且磁盘配额功能也只有在 NTFS 卷上才能发挥作用。管理员可以根据需要为各个用户设置不同的配额限度或警告级别，也可以为还没有在卷上复制、保存过文件或取得文件所有权的用户设置配额，或者在一个新建的空白卷上启用磁盘配额。

磁盘配额功能在启用时需要设定两个值：磁盘配额空间限制和磁盘配额警告级别。磁盘配额空间限制用于指定允许用户使用的最大磁盘空间容量(一般情况下应当配置为当用户试图使用的空间大小超出限制时将被禁止，并由系统记录该事件，当然也可以配置为当用户超出限制时仍可继续使用，仅由系统记录该事件，供管理员根据记录信息进行跟踪和调整)。磁盘配额警告级别指定了用户接近其配额限度的值。通常配置下，当用户对卷空间的使用超过配额警告级别时，系统就会记录该事件。

2.3.2　磁盘配额的设置

对于已经创建好 NTFS 的卷，启动磁盘配额的方法非常简单，只需由管理员在“计算机”窗口中右击相应的卷标，在弹出的快捷菜单中选择“属性”命令，在弹出的“属性”对话框中单击打开“配额”选项卡，如图 2-34 所示，然后选中“启用配额管理”复选框，再单击“确定”按钮或“应用”按钮即可。

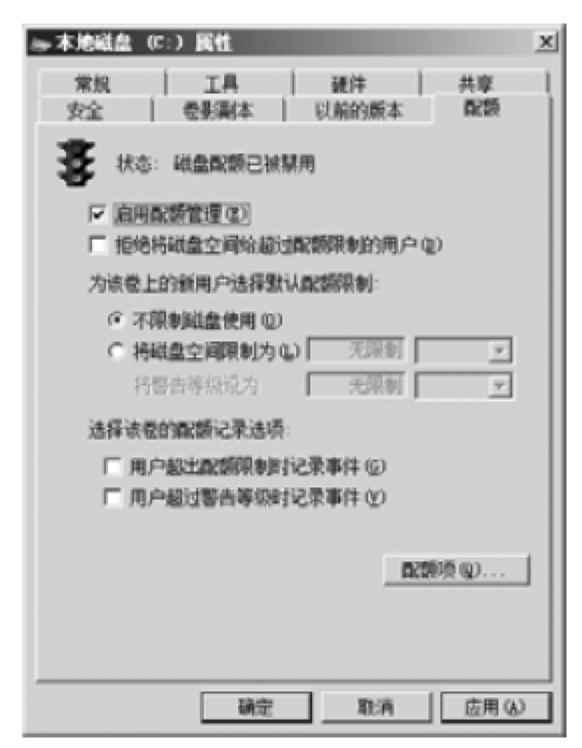


图 2-34　启用磁盘配额管理

当管理员针对某个卷启用磁盘配额后，Windows Server 2008 就会计算到启动启用磁盘配额功能时刻为止在该卷中复制文件、保存文件或取得文件所有权的用户使用过的磁盘空间，然后根据计算结果自动为每个用户指定配额限度和警告级别。这些工作将导致卷重新被扫描，以便将磁盘使用方式数据更新到最新状态。因此当管理员启用磁盘配额时，系统会弹出如图 2-35 所示的信息提示对话框让管理员再次确认。

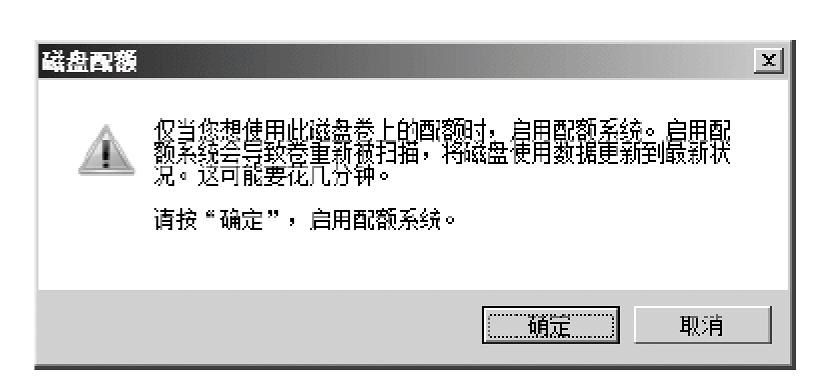


图 2-35　启用磁盘配额-再次确认

磁盘配额在卷上启用以后，就可以通过“配额”选项卡上的“配额项”按钮查看当前在卷上已经复制、保存过文件或取得文件所有权的用户列表，以及每个用户的卷空间使用量、当前设定的配额限制、警告等级及已使用空间的百分比等信息，如图 2-36 所示。如果要调整某个用户的配额属性，只需在该列表中双击相应用户所在的行，然后弹出该用户在当前 NTFS 卷上的“磁盘配额设置”对话框，如图 2-37 所示，在对话框中为用户设置新的磁盘空间限制大小和警告等级大小即可。也可以根据需要将用户设定为“不限制磁盘使用”。

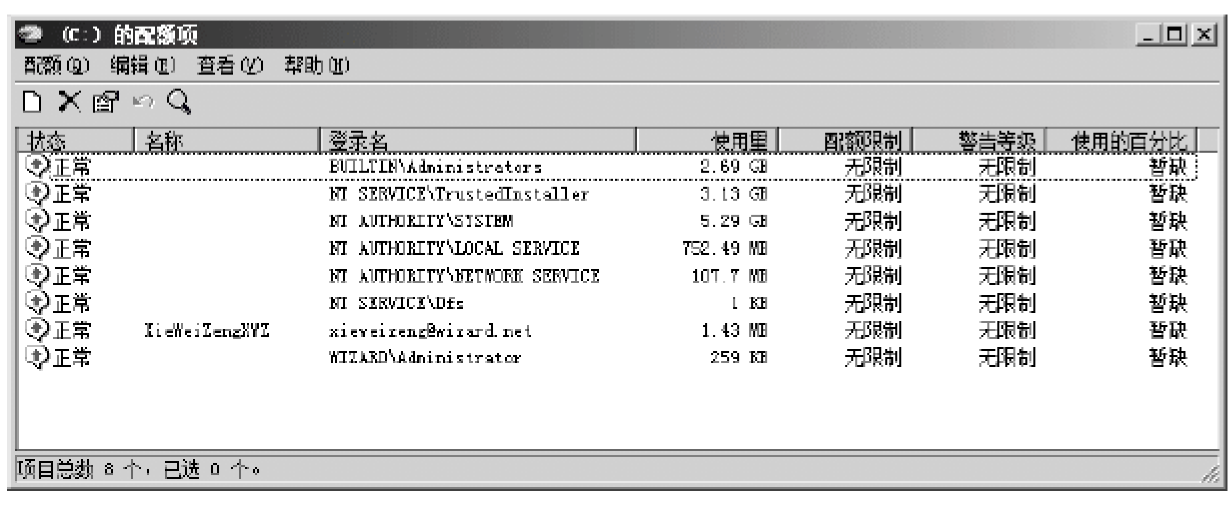


图 2-36　配额项窗口



图 2-37　配额设置对话框

对于新用户(即尚未在卷上复制、保存过文件或取得文件所有权的用户)来说，也可以在“属性”对话框的“配额”选项卡中为其指定默认的配额限制。在此处还可以对当前卷的整体配额记录选项(即用户超出配额限制时是否记录事件、用户超过警告等级时是否记录事件)进行设置，并规定当用户超出配额限制时是否拒绝分配磁盘空间。

如果某个用户在启用磁盘配额管理的 NTFS 卷上使用的空间超出了管理员给其指定的磁盘配额警告级别，那么该用户在该卷配额项列表中就会显示为警告状态，如图 2-38 所示。如果当前卷的配额记录方式设定为“用户超过警告等级时记录事件”，则系统也会自动记录该事件的相关信息，如图 2-39 所示，以供管理员在事件查看器中查看。如果磁盘配额设置为“拒绝将磁盘空间给超过配额限制的用户”，则当用户要占用的空间超过管理员给其指定的磁盘空间限制时，系统会自动拒绝用户对空间的占用，并显示如图 2-40 所示的空间不足的警告信息。信息上所显示的磁盘空间总大小就是管理员给用户指定的磁盘空间限制大小。

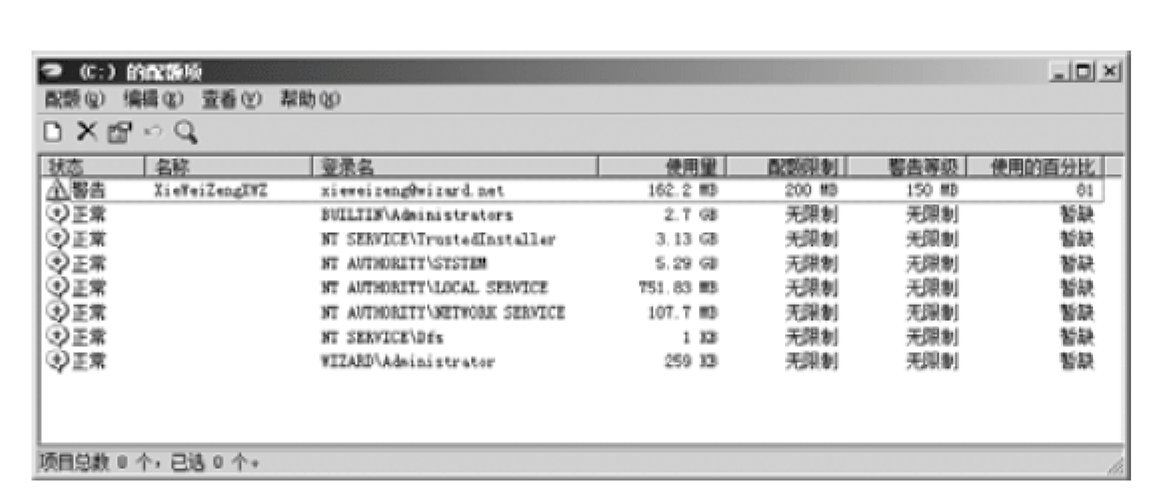


图 2-38　磁盘配额设置-警告状态



图 2-39　磁盘配额设置-事件属性



图 2-40　磁盘配额设置-空间不足信息

2.4　分布式文件系统

2.4.1　分布式文件系统概述

大多数网络环境中，共享资源都驻留在多台服务器上的各个共享文件夹中。要访问资源，用户或程序必须通过驱动器映射等方式连接到共享资源所在的服务器。当访问不同的资源时需要分别访问不同的服务器。通过分布式文件系统(Distributed File System，DFS)，一台服务器上的某个共享点能够作为驻留在其他服务器上的共享资源的宿主。DFS 以透明方式链接文件服务器和共享文件夹，然后将其映射到单个层次结构，以便可以从一个位置对其进行访问，而实际上数据却分布在不同的位置。用户不必再转至网络上的多个位置以查找所需的信息，而只需连接到 DFS 的根目录，然后在访问根目录所包含的文件夹时将被自动重定向到包含相应共享资源的网络位置。这样，用户只需知道 DFS 根目录共享即可访问整个网络环境的共享资源。

Windows Server 2008 中的分布式文件系统包括两种技术，可以同时使用或分别使用这两种技术，在基于 Windows 的网络上提供容错且灵活的文件共享和复制服务。

1. DFS 命名空间(DFS Namespace)

使用 DFS 命名空间，可以将位于不同服务器上的共享文件夹组合到一个或多个逻辑结构的命名空间。每个命名空间作为具有一系列子文件夹的单个共享文件夹显示给用户。命名空间的基本结构可以包含位于不同服务器以及多个站点中的大量共享文件夹。由于共享文件夹的基本结构对用户是隐藏的，因此 DFS 命名空间中的单个文件夹可与多个服务器上的多个共享文件夹相对应。此结构可提供容错功能，并能够将用户自动连接到本地共享文件夹(可用时)，而不是通过广域网(WAN)连接对这些用户进行路由。

2. DFS 复制(DFS Replication)

DFS 复制是一个多主机复制引擎，使用该引擎，用户可以通过局域网或广域网(WAN)网络连接同步多个服务器上的文件夹。它使用远程差分压缩(RDC)协议仅更新自上次复制后已更改的那部分文件内容。

Windows Server 2008 中的分布式文件系统是作为文件服务角色的角色服务实施的。对应于它所包含的两种技术，分布式文件系统包含两种角色服务：DFS 命名空间和 DFS 复制。安装“文件服务”服务器角色的过程中选择安装“DFS 命名空间”和“DFS 复制”这两种角色服务即可使服务器具备 DFS 的功能。如图 2-41 所示，表示“DFS 命名空间”与“DFS 复制”已安装成功并正在运行。



图 2-41　DFS 服务安装成功正常运行

若要管理运行 Windows Server 2008 的计算机上的 DFS 命名空间和 DFS 复制，可以使用由服务器管理器承载的“DFS 管理”管理单元，也可以使用“管理工具”文件夹中的“DFS 管理”管理单元(DFS Management)。“DFS 管理”管理单元界面如图 2-42 所示。



图 2-42　“DFS 管理”管理单元界面

2.4.2　添加 DFS 映射

DFS 命名空间可以在安装 DFS 角色服务的时候由安装向导提示创建，也可以在以后根据需要通过“DFS 管理”管理单元新建。只有创建了 DFS 命名空间，才能通过向命名空间中添加共享文件夹的方法来添加 DFS 映射。

DFS 命名空间中的共享文件夹都需要管理员手动添加以创建连接。需要注意的是，添加到命名空间的共享文件夹，其共享属性和访问权限必须是事先指定好的，创建连接并不能自动创建共享文件夹，它只是建立一个目标文件夹映射而已。

新建一个 DFS 命名空间的过程如下：

(1) 通过“DFS 管理”管理单元的“新建命名空间”操作启动“新建命名空间向导”，如图 2-43 所示。

(2) 在向导对话框中输入承载该命名空间的服务器的名称，然后在下一页输入要创建的新命名空间的名称。如有必要，还可以单击“编辑设置”按钮，在弹出的“编辑设置”

对话框中指定新命名空间所包含的共享文件夹的本地路径及共享权限，如图 2-44 所示。

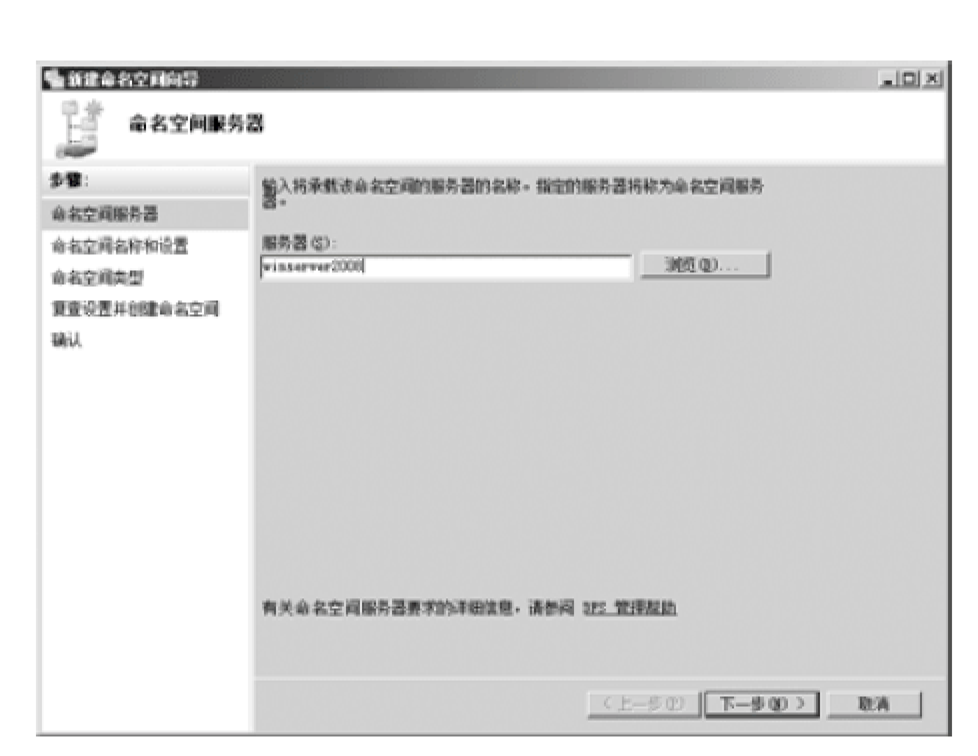


图 2-43　新建命名空间向导



图 2-44　新建命名空间向导-“编辑设置”对话框

(3) 下一步选择要创建的命名空间类型，如图 2-45 所示。类型必须是下列两种之一：

① 独立命名空间。如果服务器上没有使用安装运行 Active Directory 域服务(AD DS)，或者希望使用故障转移集群提高命名空间的可用性，应选择此类型；

② 基于域的命名空间。如果希望使用多个命名空间服务器来确保命名空间的可用性，并且希望对用户隐藏命名空间服务器的名称，使得更易于替换命名空间服务器或将命名空间迁移到另一台服务器，应选择此类型。另外，如果选择基于域的命名空间，还必须选择命名空间模式是 Windows 2000 Server 模式还是 Windows Server 2008 模式。

(4) 最后检查前面各步骤所做的设置，如果没有问题，单击“创建”按钮即可创建新的命名空间。



图 2-45　新建命名空间向导-命名空间类型

在创建命名空间后，就可以将各服务器中创建的共享文件夹添加到命名空间中统一管理和使用了。具体步骤如下：

(1) 打开“服务器管理器”中的“DFS 管理”管理单元，选中命名空间，以列出当前服务器的 DFS 中已创建的命名空间。

(2) 在想要添加共享文件夹的命名空间上右击，从弹出的快捷菜单中选择“新建文件

夹”命令，或直接选择窗口右部的“新建文件夹”操作链接，弹出如图 2-46 所示的“新建文件夹”对话框。



图 2-46　创建 DFS 映射-“新建文件夹”对话框

(3) 在“新建文件夹”对话框的“名称”文本框中输入要添加的 DFS 映射的新名称，如图 2-46 中的“ShareFiles”。

(4) “新建文件夹”对话框的文件夹目标列表框将显示出已经添加的共享文件夹的位置及名称。要添加共享文件夹，还需单击“添加”按钮，弹出“添加文件夹目标”对话框，如图 2-47 所示。在添加共享文件夹时，还可以通过单击“添加文件夹目标”对话框中的“浏览”按钮，打开“浏览共享文件夹”对话框，如图 2-48 所示，在此对话框中浏览域中各个服务器所提供的共享文件夹，并选择需要的进行添加。此处可以添加不同服务器上的不同共享文件夹，如图 2-46 中所显示的情况，将服务器 winserver2008 上的共享文件夹 Audio 和服务器 newserver 上的共享文件夹 pdf，一并映射到了 wizard.net 域中的 NewSpace 命名空间里新建的 ShareFiles 共享文件夹中。

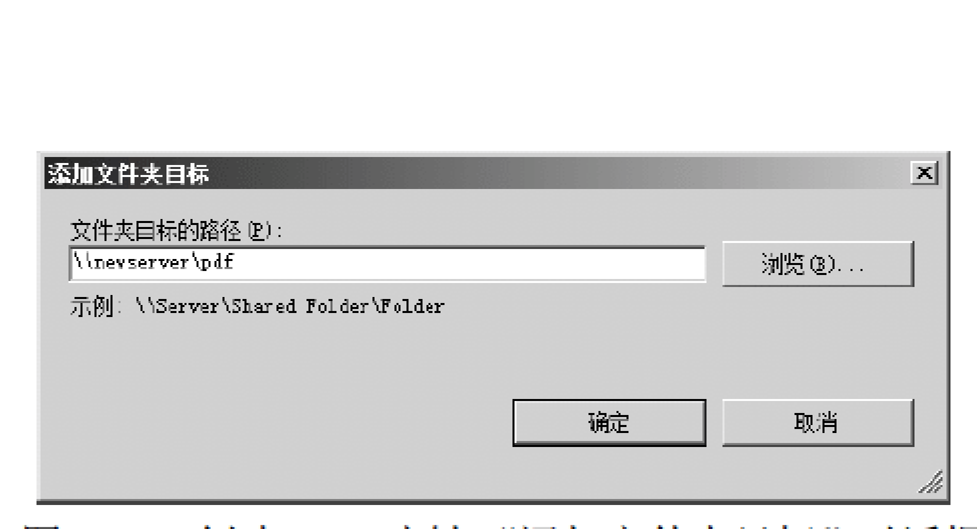


图 2-47　创建 DFS 映射-“添加文件夹目标”对话框



图 2-48　创建 DFS 映射-“浏览共享文件”夹对话框

(5) 设置完成后，单击“新建文件夹”对话框中的“确定”按钮，即可完成 DFS 映射的添加，新添加的映射以文件夹的形式出现在命名空间中。

2.4.3　创建 DFS 复制组

实际上一旦管理员添加完新的 DFS 映射，系统就会马上提示是否创建复制组，以用于同步刚创建的文件夹的文件夹目标，如图 2-49 所示。DFS 复制是一个基于状态的多主机复制引擎，使用许多复杂的进程来保持多个服务器上的数据同步，能够保证在一个成员上进行的任何更改均能复制到复制组的其他所有成员上。

DFS 复制支持复制计划和带宽限制，能够在有限带宽网络上更新文件，同时检测文件中数据的插入、删除和重新排列，很好地解决了文件冲突问题并具备自我修复能力，因此通过 DFS 复制来保证数据的有效性和一致性是很有必要的。

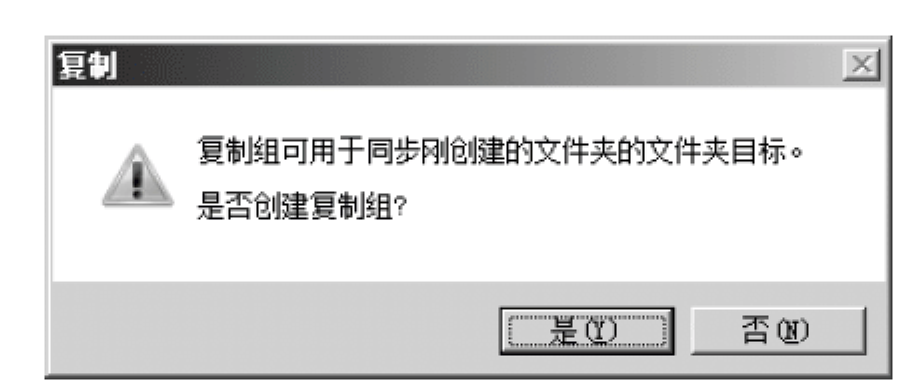


图 2-49　是否创建复制组提示框

要使用 DFS 复制发布数据，需要创建一个 DFS 复制组，然后选择包含一个或两个中心服务器(用于冗余)的集散拓扑。具体步骤如下：

(1) 打开“管理工具”中的“DFS 管理”窗口，右击“复制”节点，在弹出的快捷菜单中选择“新建复制组”命令，或在窗口右部单击“新建复制组”链接，打开如图 2-50 所示的“新建复制组向导”对话框。在第一步“复制组类型”中选中“多用途复制组”单选按钮，然后单击“下一步”按钮。

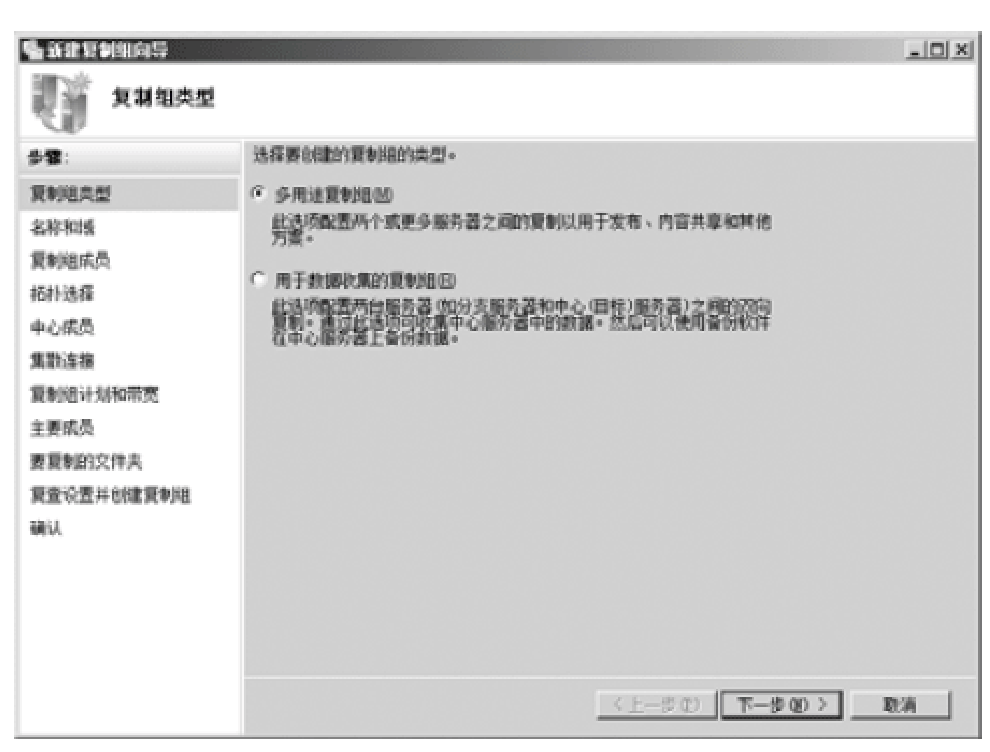


图 2-50　“新建复制组向导”对话框

(2) 在下一步骤“名称和域”中指定复制组的名称及其所在的域，如图 2-51 所示，如有需要，还可添加关于复制组的描述信息。需要注意的是，在同一个域中复制组的名称必须是唯一的。



图 2-51　新建复制组向导-名称和域

(3) 进入“复制组成员”步骤，在此处选择两个或更多将成为复制组成员的服务器，如图 2-52 所示。服务器必须先安装 DFS 复制服务才能成为复制组成员。



图 2-52　新建复制组向导-复制组成员

(4) 单击“下一步”按钮，在“拓扑选择”中选定复制组成员之间的连接拓扑，如图 2-53 所示。



图 2-53　新建复制组向导-拓扑选择

拓扑类型主要有两种：

① 集散。这种拓扑类型需要 3 个或更多成员。对于每个轮辐成员，需要选择必需的中心成员和(可选)用于冗余的第二个中心成员。可选中心可以确保轮辐成员在一个中心成

员不可用时仍可以复制。如果指定两个中心成员，中心成员之间将采用交错拓扑。

② 交错。在这种拓扑类型中，每个成员将与复制组的其他所有成员进行复制。如果复制组中的成员等于或少于十个，此拓扑非常适合。

如果现在选择“没有拓扑”，那么复制将不会发生，直到管理员创建了与复制组相关的其他自定义拓扑为止。

(5) 单击“下一步”按钮，在“复制组计划和带宽”中可以选择使用指定带宽进行全天候复制，还是在指定的日期和时间进行复制，如图 2-54 所示。如果选择在指定的日期和时间进行复制，还可以单击“编辑计划”按钮，在弹出的“编辑计划”对话框中，进一步选择用于复制的具体时间和带宽使用率，如图 2-55 所示。

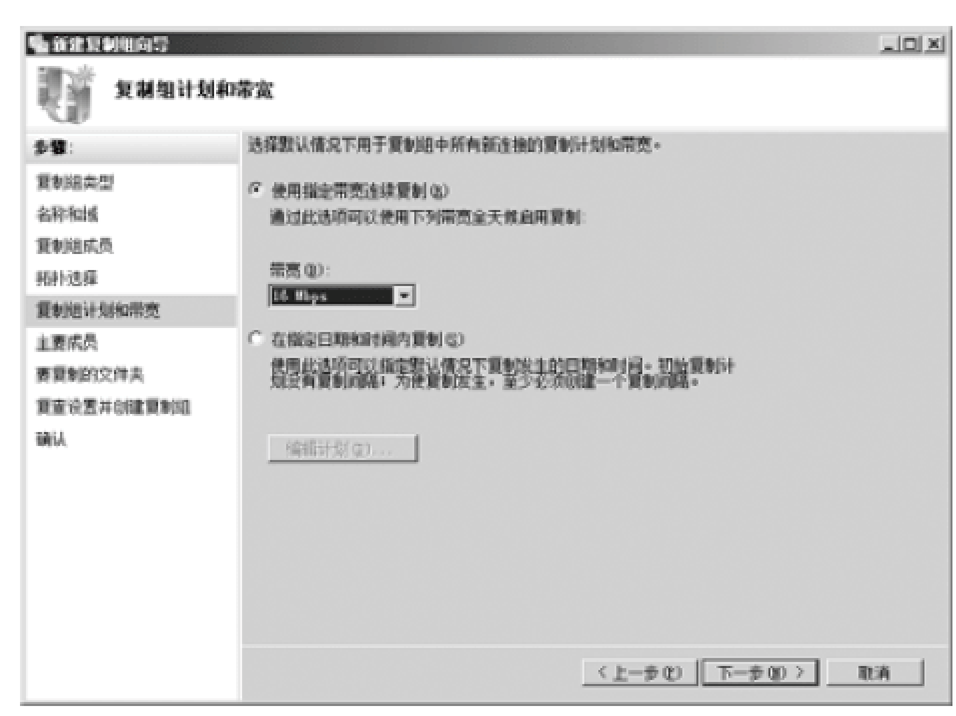


图 2-54　新建复制组向导-复制组计划和带宽

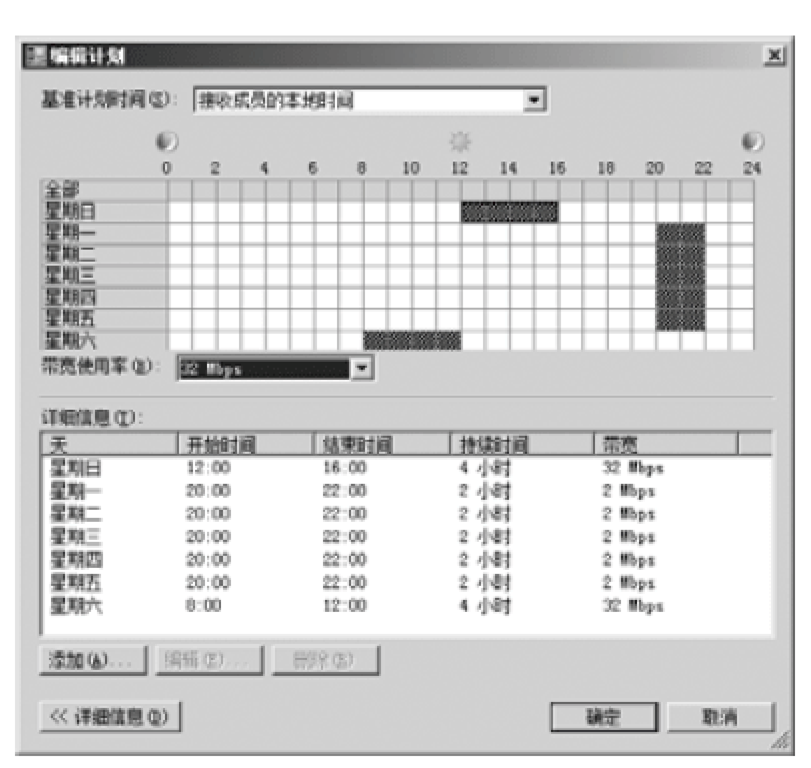


图 2-55　新建复制组向导-“编辑计划”对话框

(6) 单击“下一步”按钮，在“主要成员”界面中，需要在复制组成员中选择一个服务器作为主要成员，如图 2-56 所示。主要成员上的文件夹和文件将在初始复制期间具有权威性。

(7) 单击“下一步”按钮，“要复制的文件夹”要求选择在主要成员中希望复制到复制组其他成员的文件夹，如图 2-57 所示。可以单击“添加”按钮，弹出“添加要复制的文件夹”对话框，如图 2-58 所示，浏览主要成员服务器上的本地资源并添加需要进行复制的文件夹，例如 C 卷上的 Audio 文件夹。此处也可以根据需要选择多个需要复制的文件夹，并分别指定它们的名称和权限。

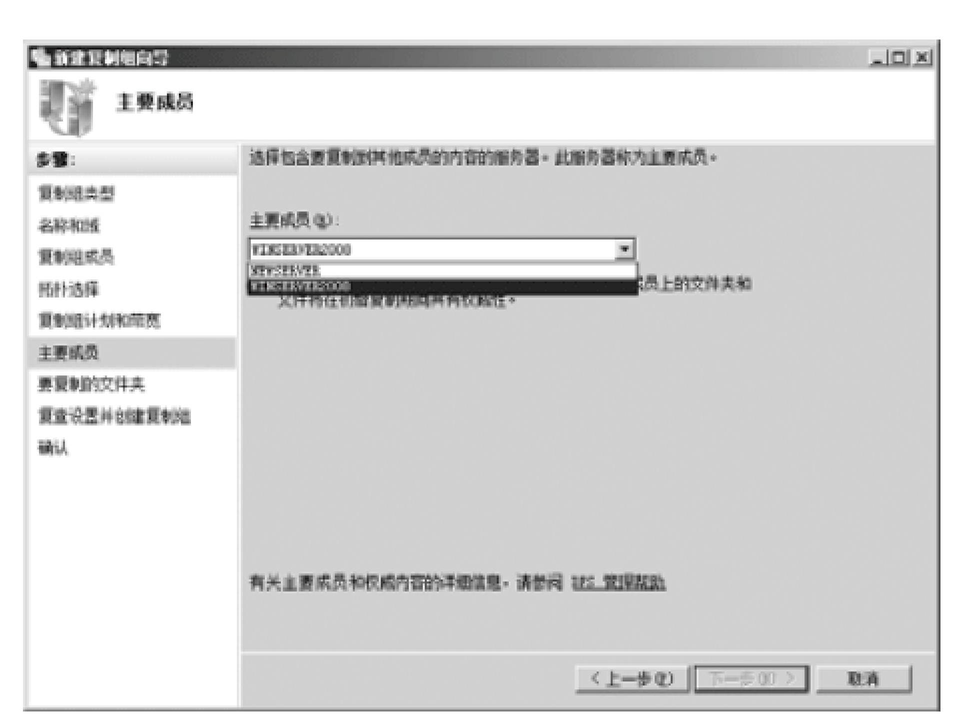


图 2-56　新建复制组向导-主要成员

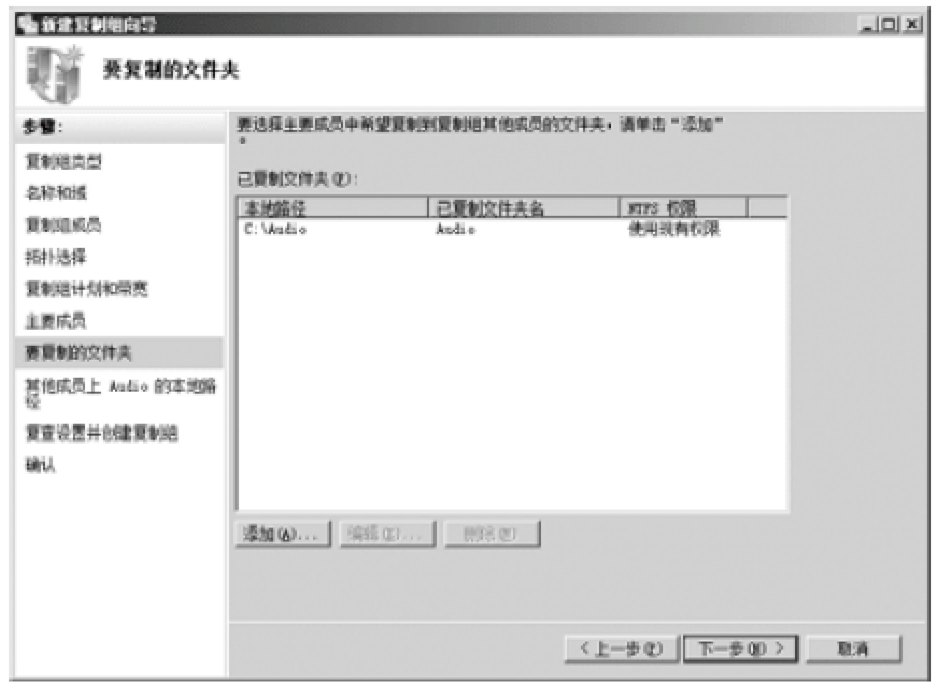


图 2-57　新建复制组向导-要复制的文件夹

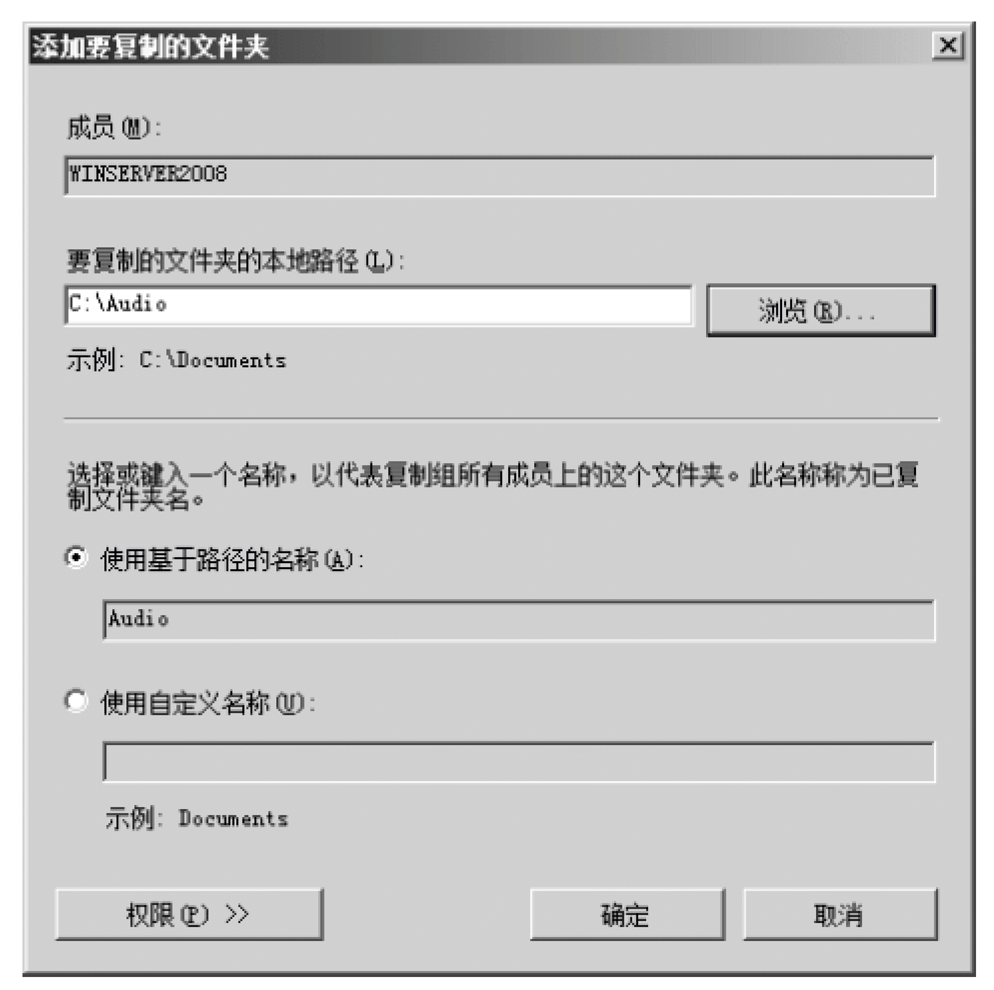


图 2-58　新建复制组向导-“添加要复制的文件夹”对话框

(8) 然后选择“其他成员上 Audio 的本地路径”，如图 2-59 所示，Audio 是上一步骤中选定的主要成员中要共享的文件夹名称，实际操作时会根据情况有不同的显示。默认情况下其他成员的本地路径是被禁用的，此时需要通过单击“编辑”按钮打开“编辑”对话框，如图 2-60 所示，选定其他成员上参与复制的文件夹的本地路径。



图 2-59　新建复制组向导-其他成员上的本地路径

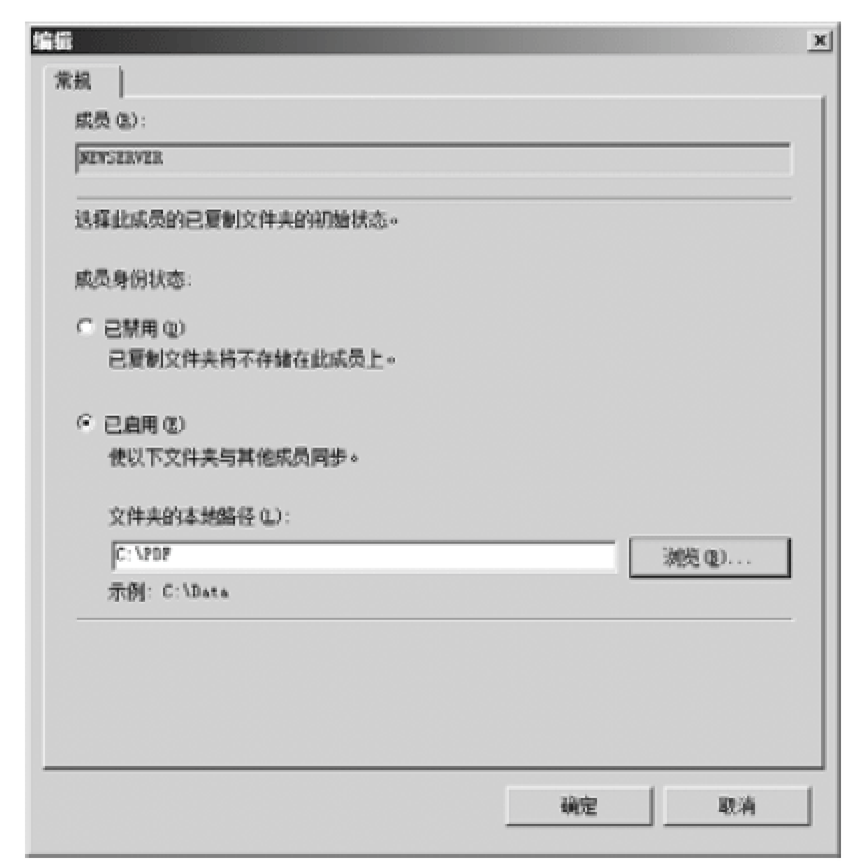


图 2-60　新建复制组向导-其他成员上的本地路径编辑对话框

(9) 返回“新建复制组向导”对话框，单击“下一步”按钮，进入“复查设置并创建复制组”步骤，如图 2-61 所示，如果各项设置经检查没有问题，单击“创建”按钮就可以真正开始复制组的创建工作。创建完毕后，系统还会显示“确认”信息，如图 2-62 所示，提示用户复制组创建的总体情况。至此 DFS 复制组创建完毕。

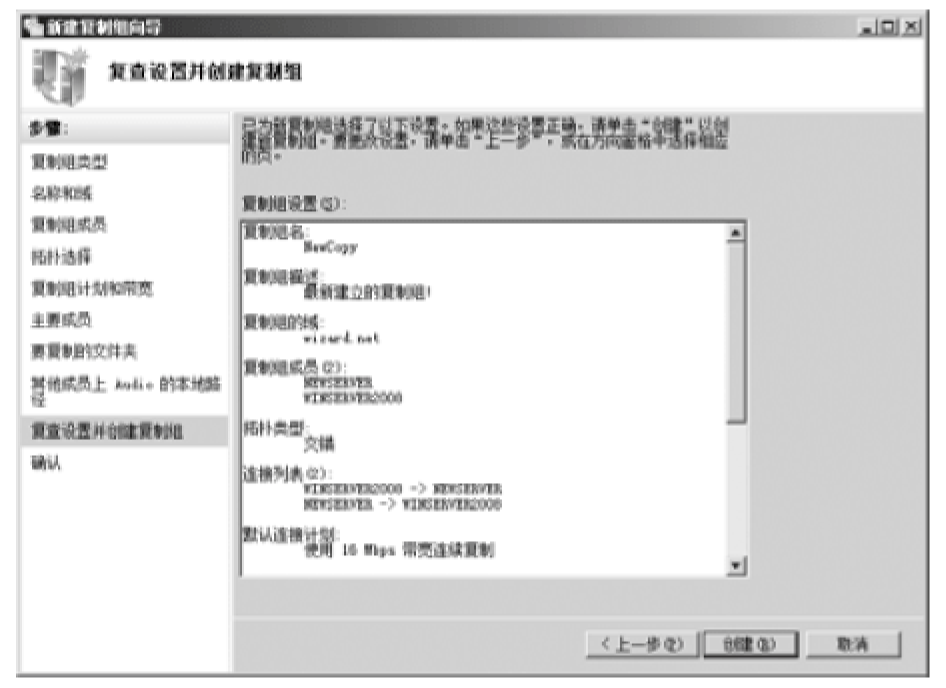



图 2-61　新建复制组向导-复查设置并创建复制组



图 2-62　新建复制组向导-确认

2.4.4　发布 DFS 复制组

为了使域中的用户能够更方便地访问复制组文件夹，还需要将 DFS 复制组发布到命名空间中。具体步骤如下：

(1) 在“服务器管理器”窗口或“DFS 管理”窗口中找到要进行发布的复制组，选中以后，在详细信息窗格中打开“已复制文件夹”选项卡，右击要共享的已复制文件夹，在弹出的快捷菜单中选择“在命名空间中共享和发布”命令，如图 2-63 所示。

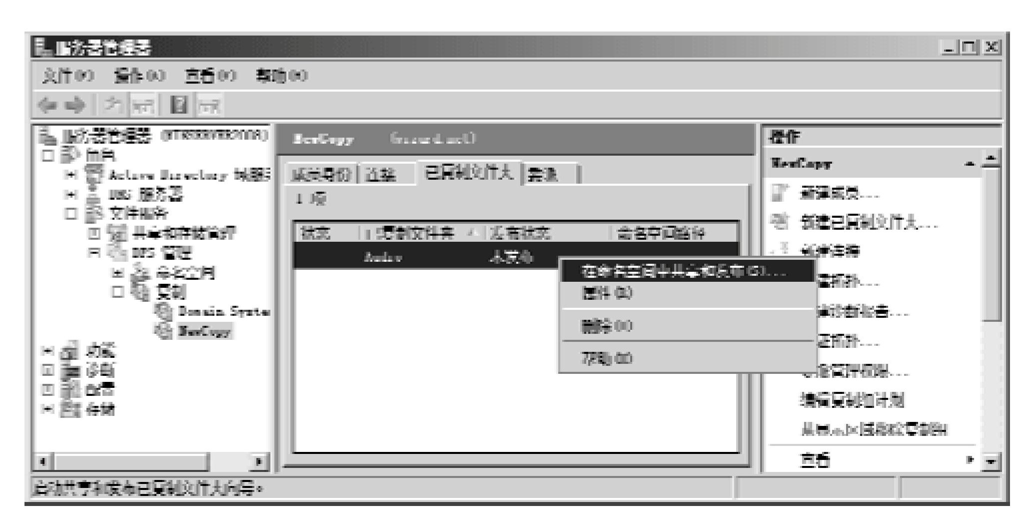


图 2-63　在命名空间中共享和发布

(2) 在弹出的“共享和发布已复制文件夹向导”对话框中首先选择发布方法，如图 2-64 所示。此处选中默认的“共享和发布命名空间中的已复制文件夹”单选按钮。

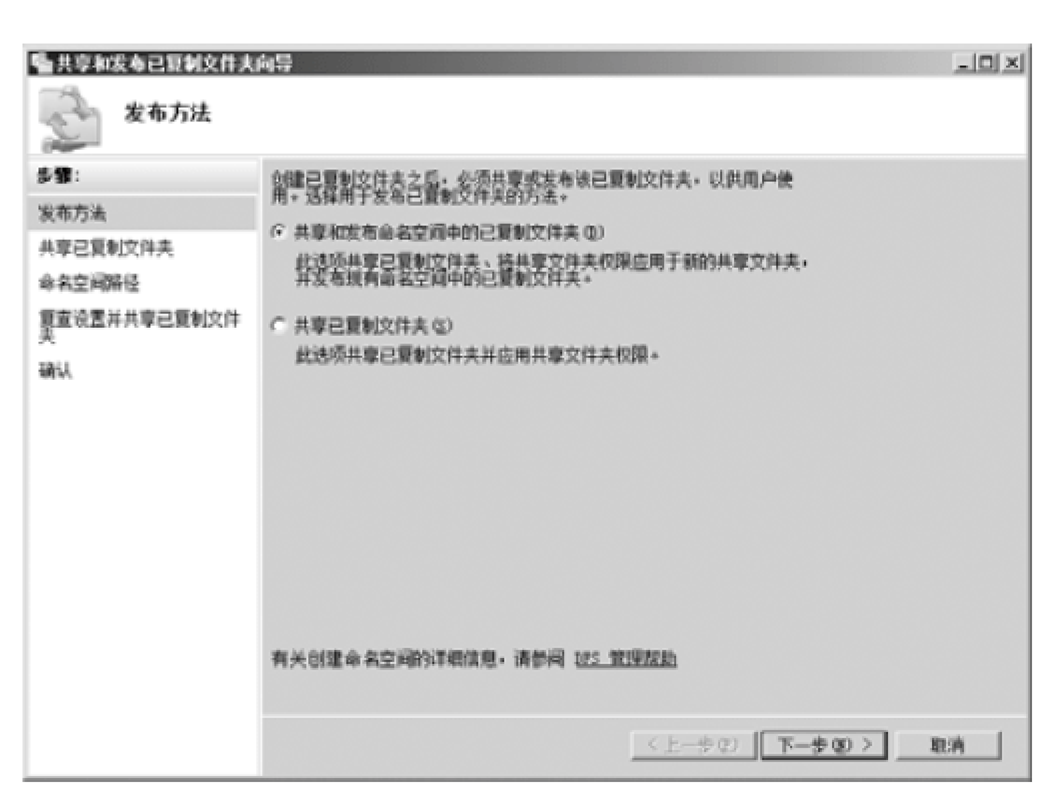


图 2-64　“共享和发布已复制文件夹向导”对话框

(3) 在“共享已复制文件夹”步骤再次审查每个已复制文件夹的“操作”列，如图 2-65 所示。如果需要共享文件夹，可以单击“编辑”按钮，弹出“编辑共享”对话框，如图 2-66 所示为已复制文件夹指定新的共享名称和共享权限。

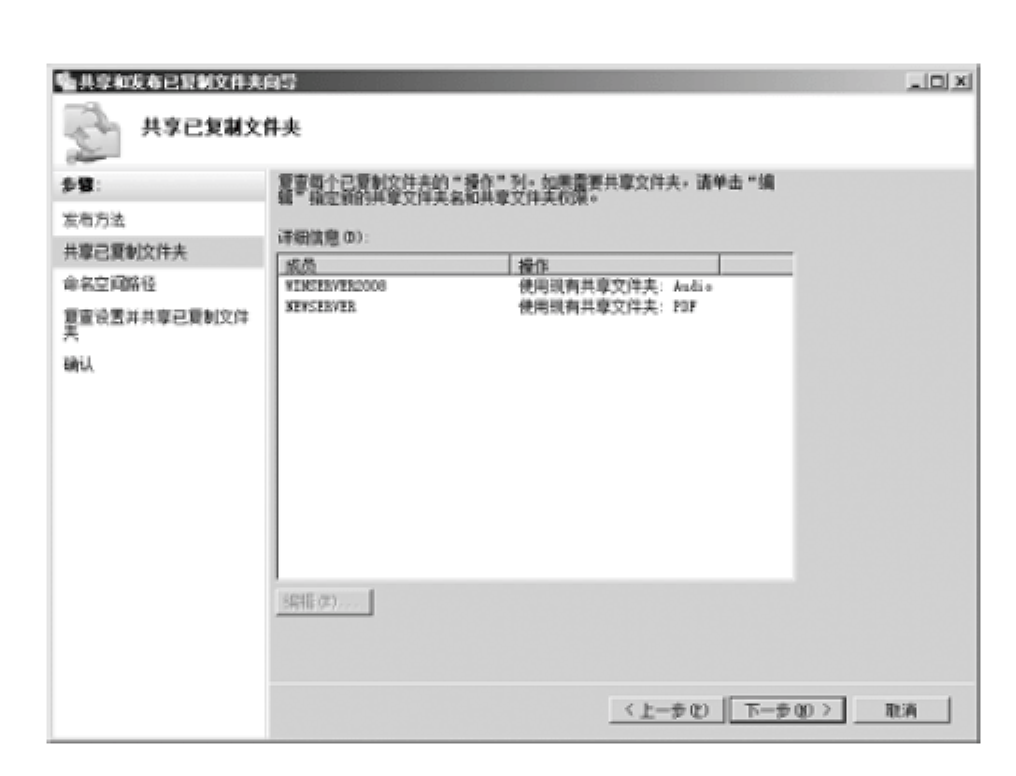


图 2-65　共享和发布已复制文件夹向导-共享已复制文件夹



图 2-66　共享已复制文件夹-“编辑共享”对话框

(4) 在下一步的“命名空间路径”中，首先需要选择当前域中的某个命名空间并指定一个父文件夹作为发布位置，然后还需要给已复制文件夹指定一个在命名空间中的新文件夹名称，如图 2-67 所示。



图 2-67　共享和发布已复制文件夹向导-命名空间路径

(5) 最后进入“复查设置并共享已复制文件夹”步骤，如图 2-68 所示，如果各项设置无误，即可单击“共享”按钮，对已复制文件夹进行共享和发布。当系统成功完成各项任务并提示信息(如图 2-69 所示)后，表明复制文件夹共享和发布成功。



图 2-68　共享和发布已复制文件夹向导-复查设置并共享已复制文件夹

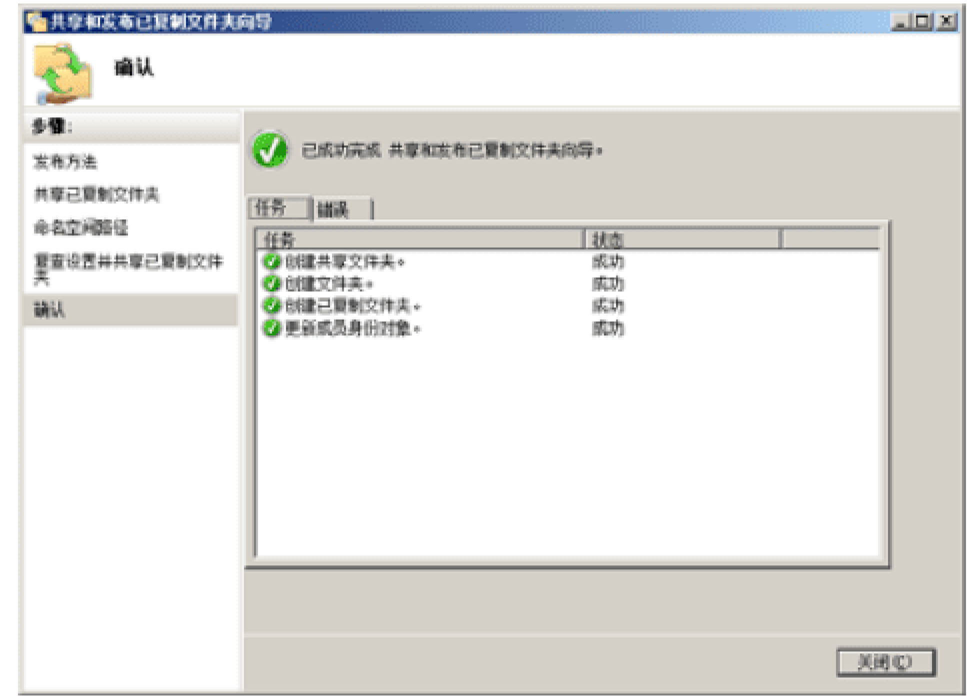


图 2-69　共享和发布已复制文件夹向导-确认

DFS 复制组发布成功以后，登录到域的用户即可通过访问域中的命名空间及设定的文件夹来访问已复制文件夹的内容了，如图 2-70 所示。



图 2-70　访问已发布的 DFS 复制组

2.5　本章小结

在 Windows Server 2008 所提供的文件服务功能中，NTFS 文件权限和共享文件夹权限可以控制用户文件的访问；分布式文件系统(DFS)通过 DFS 命名空间和 DFS 复制提供了灵活的文件共享和复制服务；磁盘配额管理确保了每个用户所使用的磁盘空间不会超过限定的阈值。除此以外，Windows Server 2008 的文件服务还提供了卷影副本和备份功能确保系统能够快速地从受损的数据和硬件故障中恢复；文件屏蔽管理功能控制用户可以保存的文件类型以及在用户尝试保存未经授权的文件时生成通知；文件分类功能自动对文件进行分类、运行报告以及对服务器上的文件应用基于分类的文件过期和自定义操作，确保管理员在有效管理数据的同时可以最大程度地减少工作量。

Windows Server 2008 的文件服务提供了从文件访问、权限控制、空间使用限制到文件同步复制、文件备份及恢复等操作的全方位功能，使得管理员能够高效、灵活地进行文件管理。其中分布式文件系统(DFS)以对用户透明的方式统一组织文件服务器和共享文件夹的文件，使用户能够极为方便地访问整个网络环境的共享资源，DFS 复制组则确保了数据文

件的有效性、一致性和安全性。

2.6　思考与练习

【思考题】

1. 在 Windows Server 2008 系统中设置资源共享有哪两种方式？每种方式需要怎样的步骤？

2. 访问网络共享资源有哪几种方法？

3. NTFS 文件夹权限有哪几种类型？

4. 在创建 DFS 复制组的过程中，复制组成员之间的连接拓扑类型主要有哪两种？各有什么特点？

【练习题】

初始条件：一台尚未启用磁盘配额管理的 Windows Server 2008 服务器、服务器管理员帐户。

操作目标：在 Windows Server 2008 服务器的所有卷上启动磁盘配额管理，并将所有新用户在该卷上可使用的磁盘空间限制设定为 500MB，警告等级设置为 450MB，并设置为记录所有的超出警告等级事件和超出配额限制事件。

第3章　信息共享服务

【本章导读】

信息共享是现代生活的基础，无论是在单位工作，还是在日常的学习和生活当中，我们都需要频繁地与他人分享信息。各种规模的组织和业务单位都需要通过信息共享来提高业务流程的效率和团队的工作效率，通过使用有助于用户跨组织和跨地区边界保持连接的协作工具来保证用户能够访问其所需的信息。微软公司开发的 Windows SharePoint Services(以下简称 WSS)提供了符合上述需求的解决方案。WSS 是一个能够用来实现信息共享和文档协作的工具，提供了大量工具以及一个伸缩性极好的、基于 Web 应用程序的通用基础平台。WSS 能够构建基于 Web 的各种应用程序，并可以轻松地调整和缩放这些程序，以满足不断变化和日益增长的业务需求。

3.1　安装 WSS 服务

3.1.1　安装前的准备

WSS 是微软公司开发的一款用于 Windows Server 2003 的免费增值软件。事实上 Windows Server 2003 R2 已经包含了它，但是 Windows Server 2008 系统并没有直接包含 WSS，用户需要到微软公司的网站免费下载。WSS 的前端是一个运行于 Internet Information Services 6.0 之上的 ASP.NET 网站，后端由 SQL Server 来存储数据。WSS 包括以下 5 个主要的模块：

- 基于 ASP.NET 2.0 平台，并提供数据库服务、文档管理、安全和访问控制以及管理功能的一套软件。
- 由一个或者多个 Internet 信息服务(IIS)Web 服务器组成的一套 Web 传输装置。
- 一个 Microsoft SQL Server 数据库。
- 在 Web 服务器上执行的 Web 部件和在 Web 页面显示数据和内容的 Web 部件。
- 协作和会议模板(网站模板)。

基于这种模块结构的要求，WSS(以 WSS 3.0 为例)必须安装在 Windows Server 2003 SP1 或更高版本的服务器操作系统上，同时还要求系统中已经安装有以下组件：

- Microsoft .NET Framework 3.0；
- SQL Server 2005(若没有安装 SQL Server 2005，也可以在安装 WSS 3.0 的时候选择完整安装，这样它就会安装一个 Express 版本的 SQL Server)；

- Internet Information Services(IIS) 6.0(包含 ASP.NET 2.0)；
- SMTP 服务器。

3.1.2　WSS 的安装

准备上述安装环境的必需组件后，下载 WSS 3.0 安装程序(可以下载包含 Service Pack 2 的完整安装包)，开始 WSS 的安装过程。

(1) 在服务器上运行 WSS 3.0 安装程序(SharePoint.exe)， 显示如图 3-1 所示的“阅读 Microsoft 软件许可证条款”对话框，选中“我接受此协议的条款”复选框，单击“继续”按钮进入下一步。

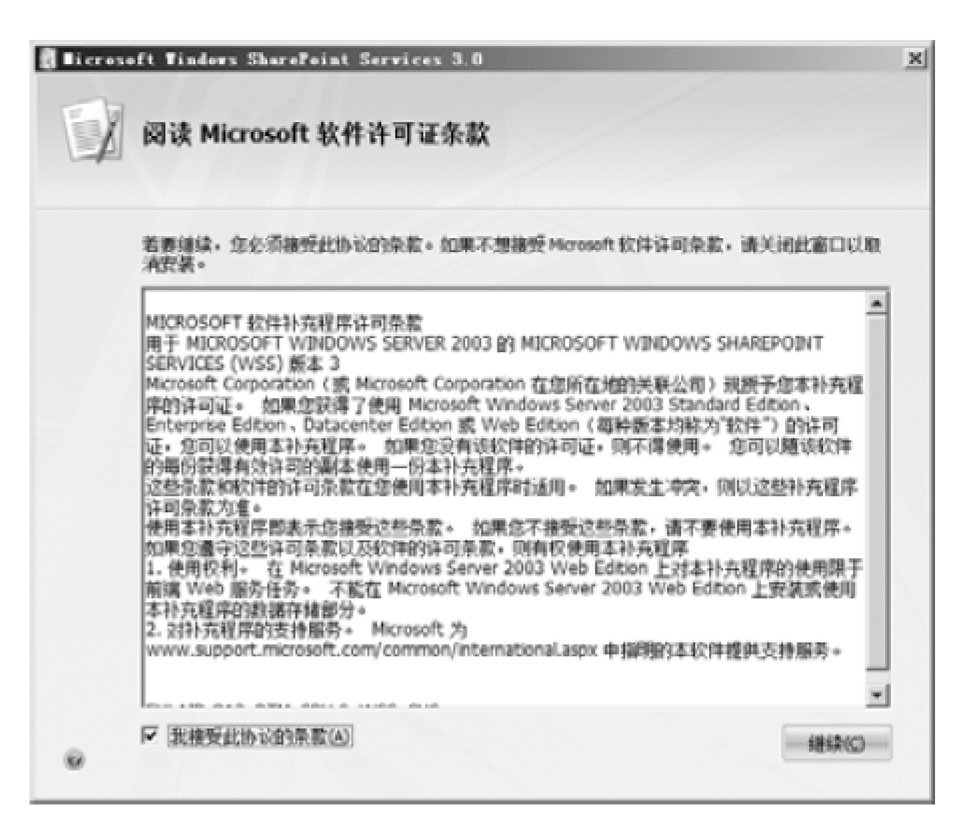


图 3-1　安装 WSS-软件许可证

(2) 在第二步“选择所需的安装”界面中，可以选择“基本”或“高级”安装模式。如果仅使用默认设置把 WSS 安装到一个独立的单服务器上，可以选择“基本”安装模式；如果要进行用户自定义设置，或进行服务器或 Share Point 场安装和设置，需要选择“高级”安装模式，如图 3-2 所示。



图 3-2　安装 WSS-选择所需的安装

(3) 如果选择“高级”安装模式，就会进入如图 3-3 所示的高级设置界面，要求管理员进一步确定服务器安装类型，此处假定选择“独立”安装类型、数据文件存放的位置以及是否参加客户体验改善计划。选择完毕后，单击“立即安装”按钮，即可开始正式安装。



图 3-3　安装 WSS-服务器类型

(4) 待安装程序完成安装后，将显示如图 3-4 所示的安装完成提示界面，但是，必须经过相应的配置以后才能让 WSS 正常工作。因此还需要选中“立即运行 SharePoint 产品和技术配置向导”复选框(也可以不选中此项，待以后根据需要再进行配置，但不推荐这样做)，然后单击“关闭”按钮关闭安装向导并启动配置向导。



图 3-4　安装 WSS-安装完成提示界面

(5) SharePoint 产品和技术配置向导的欢迎界面如图 3-5 所示。单击“下一步”按钮继续。



图 3-5　配置 WSS-欢迎界面

(6) 在开始配置前，系统再次提示配置期间可能需要启动或重置的服务清单，如图 3-6 所示，由管理员决定是否进行配置。

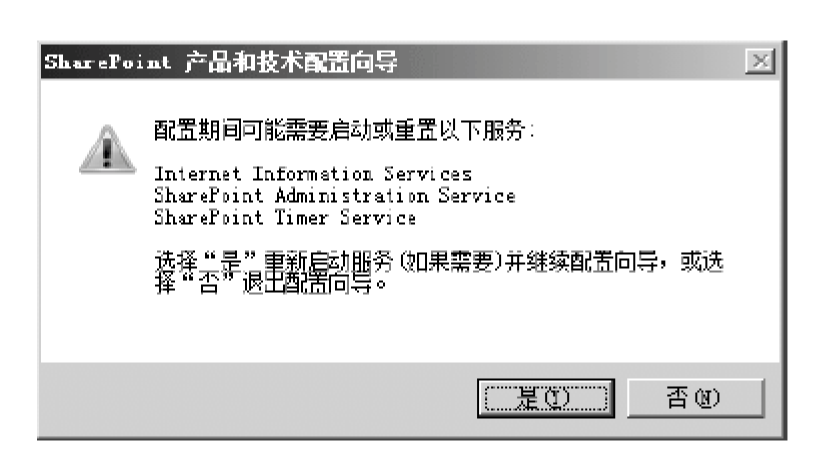


图 3-6　配置 WSS-警告信息

(7) 单击"是"按钮后，显示如图 3-7 所示的"正在配置 SharePoint 产品和技术"界面，开始配置 SharePoint。配置过程共包含 10 项配置任务。



图 3-7　配置 WSS-正在配置 SharePoint 产品和技术

(8) 配置完成后，会显示如图 3-8 所示的"配置成功"对话框，单击"完成"按钮结束 WSS 的配置过程。



图 3-8　配置 WSS-配置成功

完成 WSS 的安装与配置后，系统会自动打开 WSS 站点的初始页面，如图 3-9 所示。从该页面上可以看出，默认是以当前登录到服务器上的管理员用户身份打开页面的，而且新建立的 WSS 站点只是一个基本框架，没有任何用户的通知、事件、日历项、任务、链接等内容，仅有一个自动生成的“Windows SharePoint Services 入门”通知消息。



图 3-9　WSS 网站默认主页

3.2　管理 WSS 站点

网络管理员对 WSS 站点的管理是通过单击在 WSS 站点首页右侧的“网站操作”按钮，从下拉菜单中选择“网站设置”实现的，选择相应选项后，会进入“网站设置”页面。WSS 将所有的管理链接都集中到这一个页面中，非常方便管理员进行设置。

3.2.1　用户和权限管理

默认情况下，只有管理员(Administrator)才有对 WSS 服务器进行访问和管理的权限，其他用户帐户对 WSS 站点的访问都将被拒绝，如图 3-10 所示。因此管理员必须及时对用户和 SharePoint 用户组进行设置和对权限进行管理，为不同的用户和 SharePoint 组赋予不同的权限，使不同的用户在访问 SharePoint 网站时能执行不同的操作。



图 3-10　用户和权限管理-拒绝访问提示

WSS 的用户和权限管理包括人员和组、网站集管理员、高级权限 3 个部分。

1. 人员和组管理

以管理员身份登录到 WSS 站点后，即可通过首页左侧的“人员和组”链接进入“人员和组管理”页面，如图 3-11 所示。默认状态下，WSS 已自动生成了以下 3 个 SharePoint 用户组：

- 工作组网站成员：该组人员拥有指定 SharePoint 网站的参与讨论权限；
- 工作组网站访问者：该组人员拥有指定 SharePoint 网站的读取权限；
- 工作组网站所有者：该组人员拥有指定 SharePoint 网站的完全控制权限。

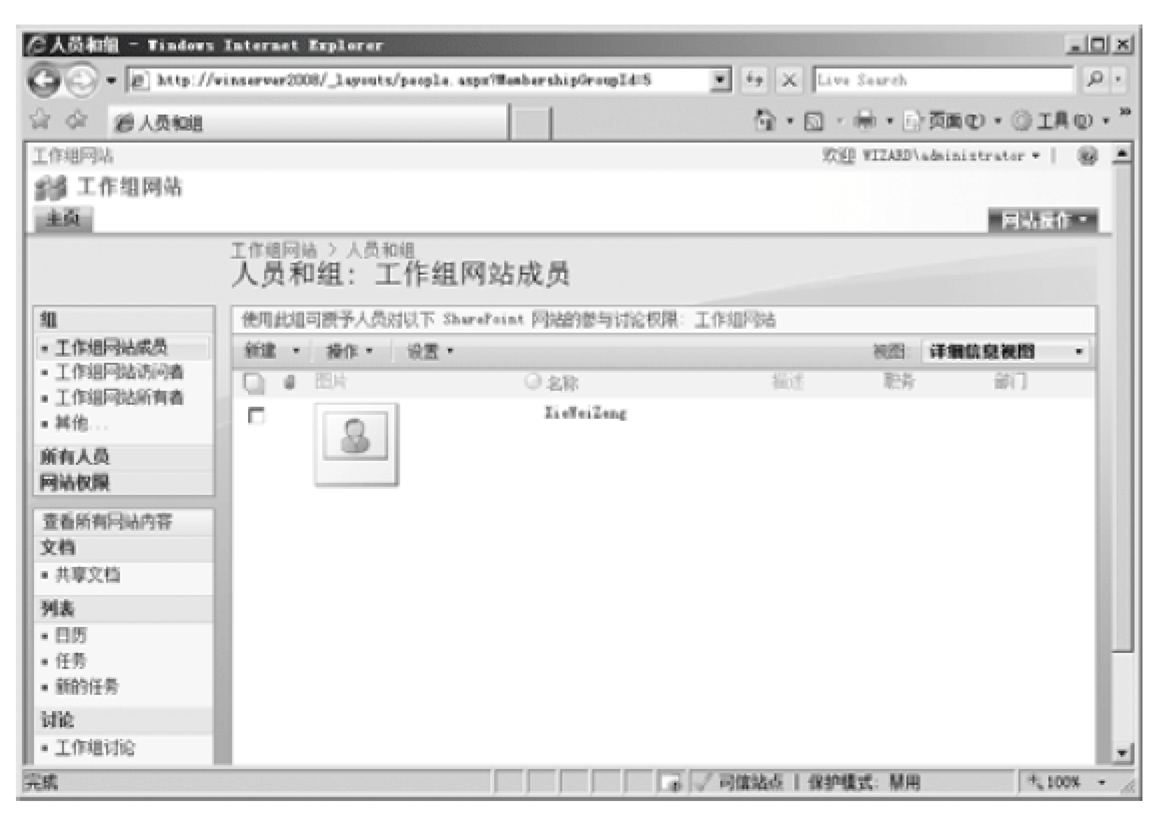


图 3-11　用户和权限管理-人员和组管理

在“人员和组管理”页面中，管理员可以根据需要查看当前某个工作组的成员，向工

作组或网站中添加用户，如图 3-12 所示，从工作组中删除用户，或对当前用户组设置进行更改，如图 3-13 所示。如果系统自动生成的 SharePoint 用户组不能满足要求，管理员还可以根据需要随时添加新的用户组并设置其属性和权限，如图 3-14 所示。



图 3-12　用户和权限管理-添加用户



图 3-13　用户和权限管理-更改用户组设置



图 3-14　用户和权限管理-新建用户组

在添加用户时，可以在添加用户界面中单击“添加所有验证用户”链接，一次性地将当前域中的所有认证用户添加到 SharePoint 用户组中，以便授予这些用户访问 WSS 网站的权限。

2. 网站集管理员管理

默认状态下，只有管理员才具有对 WSS 站点的所有网站拥有完全控制权限。但是，仅由管理员来完成所有的网站管理工作显然工作量太大，为此管理员可以将自己所信任的域用户添加为网站集管理员，由这些网站集管理员协助进行管理，如图 3-15 所示。管理员可以根据需要添加多个网站集管理员，但是需要注意的是，只能添加单个用户，而不能将用户组添加为网站集管理员。



图 3-15　用户和权限管理-网站集管理员

3. 高级权限管理

高级权限管理主要以权限管理为主。管理员可以通过高级权限管理来编辑用户组的权限，甚至是完全删除其权限，如图 3-16 所示；也可以通过“设置”菜单下的“权限级别”命令来配置当前网站上的可用权限级别。如果当前可用的权限级别不能满足要求，管理员可以通过单击“添加权限级别”链接切换到“添加权限级别”页面，如图 3-17 所示，自定义新的权限级别，以便给用户和用户组提供新的权限设置选项。



图 3-16　用户和权限管理-修改工作组权限



图 3-17　用户和权限管理-添加权限级别

3.2.2　外观管理

外观管理的目的是使 WSS 网站的外观更加符合组织的要求，以便在 WSS 站点中能够体现出企业、公司或组织的相关信息。外观管理主要包括以下 5 个方面的内容。

1. 标题、说明和图标

用来设置网站的标题和说明。标题将显示在网站的每一页中；说明将显示在主页上；图标是显示在标题旁的小图像，一般用来显示企业、公司或组织的徽标。设置页面如图 3-18 所示。如图 3-19 所示是设置标题说明和图标以后的网站首页。

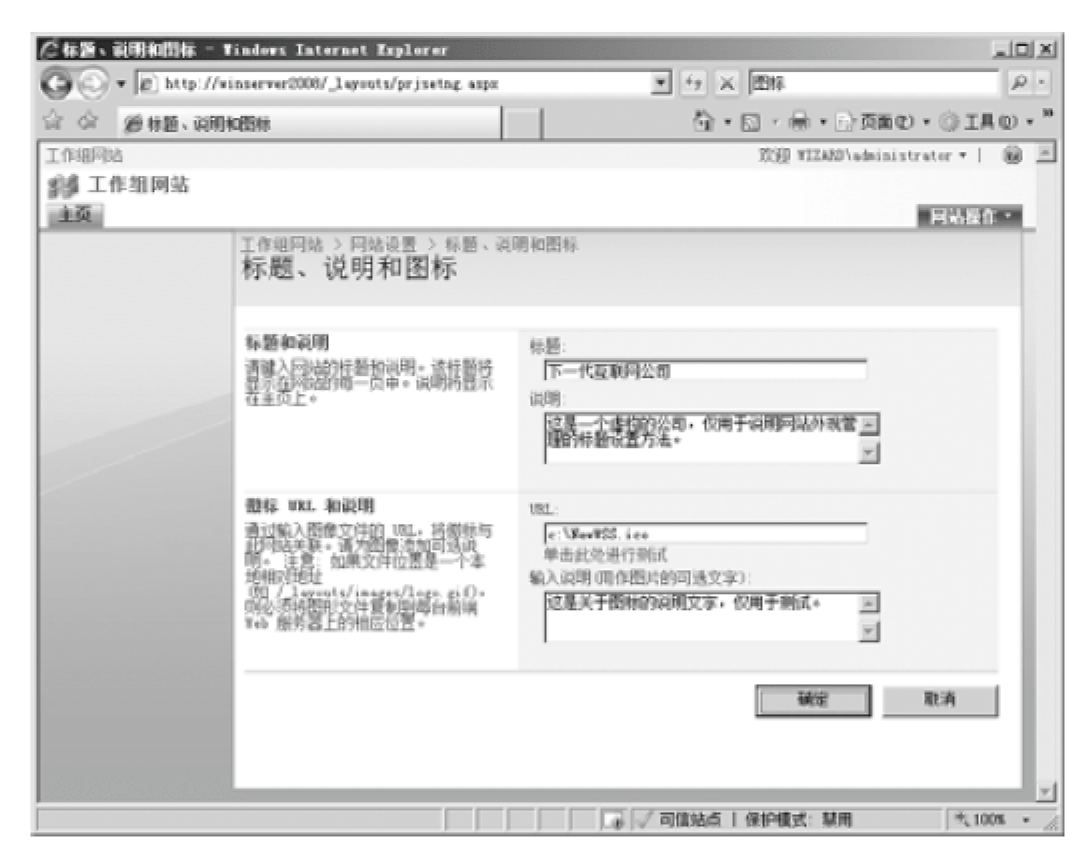


图 3-18　外观管理-标题、说明、图标设置



图 3-19　外观管理-设置标题、说明、图标后的网页效果

2. 树视图

在网站设置的“树视图”页面中，管理员可以设置用户页面的左侧显示为“快速启动”栏还是“树视图”，或者两种都显示，如图 3-20 所示。



图 3-20　外观管理-启用树视图

3. 网站主题

通过使用网站主题，可以利用系统内置的若干种主题形式来迅速改变网站整体的字体和配色方案，在网站主题设置页面，如图 3-21 所示，管理员可以从众多主题中进行选择并预览效果，如果觉得所选主题合适，单击“应用”按钮即可将该主题应用到整个网站。



图 3-21　外观管理-网站主题

4. 顶部链接栏

通过“顶部链接栏”设置功能(如图 3-22 所示)，管理员可以查看当前已有的顶部链接，建立新的顶部链接，删除现有链接或更改现有各链接的显示顺序。如图 3-23 所示的是添加了两个顶部链接栏后的网站首页。



图 3-22　外观管理-顶部链接栏设置



图 3-23　外观管理-添加顶部链接栏后的效果

5. 快速启动

“快速启动”设置功能允许管理员根据需要将新的链接或标题添加到“快速启动”栏的相应位置，以方便用户在浏览网页时迅速访问链接或标题内容。该设置页面如图 3-24 所示。



图 3-24　外观管理-快速启动设置

3.2.3　网站管理

网站管理是 WSS 网站设置的重要内容，主要包括以下 5 个方面的内容。

1. 区域设置

“区域设置”页面允许管理员指定 WSS 网站的日期、数字和排序方式所基于的区域设置，同时还可设定日历的类型、工作周的星期范围及所用的时间格式等，如图 3-25 所示。



图 3-25　网站管理-区域设置

2. 网站库和列表

在如图 3-26 所示的“网站库和列表”设置页面中，管理员可以针对当前列表中的各个项目(如共享文档、链接、任务、日历等)进行单独的自定义设置，或者在列表中添加新的项目，如通知、联系人、问题跟踪、调查等。下面以自定义“日历”设置为例，如图 3-27 所示，管理员不仅可以设置日历显示的标题、说明信息和导航方式等，还可以对日历进行各种高级设置。



图 3-26　网站管理-网站库和列表



图 3-27　网站管理-自定义日历

3. 搜索可见性

“搜索可见性”设置功能可以让管理员决定是否允许网站显示在搜索结果中，并指定是否为 ASPX 页面编制索引，如图 3-28 所示。



图 3-28　网站管理-搜索可见性

4. 网站和工作区

WSS 站点由顶级网站(处于一个网站集的层次结构顶部的网站)和子网站(顶级网站的指定子目录中存储的完整网站)构成。它们将网站内容划分为多个可进行单独管理的不同子网站。一个顶级网站可有多个子网站，子网站本身也可以有多个子网站。这种层次结构使整个工作组拥有一个主要的工作网站，并且附属项目还有单独的工作网站或共享网站。顶级网站和子网站允许对网站的功能和设置进行不同级别的控制。网站管理员控制创建、访问网站内容以及为网站添加内容的权限。

工作区实质上是一种类型独特的网站，它为工作组成员提供了文档协作或会议相关资源的协作工具及服务。工作区可以包含一些信息列表，比如相关的文档、工作组成员和链接。

通过“网站管理”功能中的“网站和工作区”管理，如图 3-29 所示，网络管理员可以对子网站和工作区进行相应的添加或删除操作，或者决定将“创建子网站”的权限添加到“设计”权限级别还是“参与讨论”权限级别。新建的 SharePoint 网站页面如图 3-30 所示。各项设置完成后，就会由 WSS 自动创建符合要求的子网站，如图 3-31 所示。该网站有自己的外观、日历和任务列表、权限设置等属性。如图 3-32 所示的是一个建好的 SharePoint 工作区(决议会议类型)。该工作区也有自己的外观、用户和权限设置等属性，同时还有与会者管理、议程管理、目标和任务管理及决议管理等符合决议会议类型特性的设置内容。



图 3-29　网站管理-网站和工作区



图 3-30　网站管理-新建 SharePoint 网站



图 3-31　网站管理-建好的 SharePoint 网站



图 3-32　网站管理-建好的 SharePoint 工作区

5. 删除此网站

当网站或工作区使用完毕，已无继续存在的必要时，就可以通过“网站管理”功能中的“删除此网站”来将其删除。删除前，系统会再次提示用户删除网站会产生的后果，如图 3-33 所示，单击“删除”按钮即可删除，否则取消删除。



图 3-33　网站管理-删除网站

3.2.4　网站集管理

网站集就是服务器上具有相同所有者且共享管理设置的一组网站。每个网站集都包含一个顶级网站，并可能包含一个或多个子网站。网站集管理为这一组网站提供了统一的管理方式，主要包括以下 3 方面内容。

1. 回收站

WSS 具有“回收站”功能。当管理员将以前建立的议程、任务、通知、目标等项目删除后，系统并非将相应的文件信息从系统中真正删除，而是先存放到回收站中。如果管理员发现进行了误删除，还可以通过“网站集管理”中的“回收站”功能找回原来的项目。如图 3-34 所示的是“回收站”页面，该页面上列出了当前网站集中所有曾被删除的项目。管理员可以根据需要选择一个或多个项目，然后单击“还原所选项目”链接进行还原，或者单击“删除所选项目”链接进行真正的删除。



图 3-34　网站集管理-网站集回收站

2. 网络层次结构

“网络层次结构”页面显示了当前网站集所包含的所有网站和工作区的层次关系，如

图 3-35 所示，管理员可以通过左侧的网站 URL 链接直接进入该网站，或者通过右侧的“管理”链接切换到相应网站的管理页面。



图 3-35　网站集管理-网站层次结构

3. 门户网站连接

如果配置“门户网站连接”(如图 3-36 所示)，可以将用户的网站连接到与 WSS 相兼容的门户网站，使用户能够对网站中的列表(如通知、任务等)进行分类、连接到用户配置文件及门户搜索服务和对其他信息进行操作。如果要配置“门户网站连接”，只需在“门户网站连接”页面中选择“连接到门户网站”，然后将门户网站的网址和名称输入相应的文本框，单击“确定”按钮即可。



图 3-36　网站集管理-门户网站连接

3.2.5　网页布局管理

默认情况下，WSS 站点的各个页面的布局已经能够满足用户的需求了，如用户主页上通知、日历项等信息，但有时候用户可能想要对页面上显示的信息作进一步的规划，以保证网页更符合自己的使用习惯和要求。

要对页面布局进行个性化设置，首先需要确保用户有足够的权限。一般情况下，网站访问者是没有权限对页面进行个性化设置的，只有网站成员或网站所有者才能进行个性化设置。对页面的个性化设置可分为两种不同的类型：一是编辑个人版本，此版本的页面设置只影响到个人用户；二是编辑共享版本，此版本的页面会影响到所有访问该页面的用户(如果用户没有设置个人版本的话)。在访问某个网页的时候，某个用户针对该网页设定的个人版本的网页布局会覆盖管理员共享版本的网页布局，除非该用户取消了对网页的个性化设置并重置网页内容。

登录到 WSS 站点后，页面的右上角会显示当前登录的用户名，在用户名上单击，然后在弹出的菜单中选择“对本页面进行个性化设置”，即可开始编辑页面的个人版本，如图 3-37 所示。如果当前登录用户拥有相应的权限(属于“网站所有者”)，在页面右侧单击“网站操作”按钮，然后选择“编辑网页”命令，即可开始编辑页面的共享版本，如图 3-38 所示。

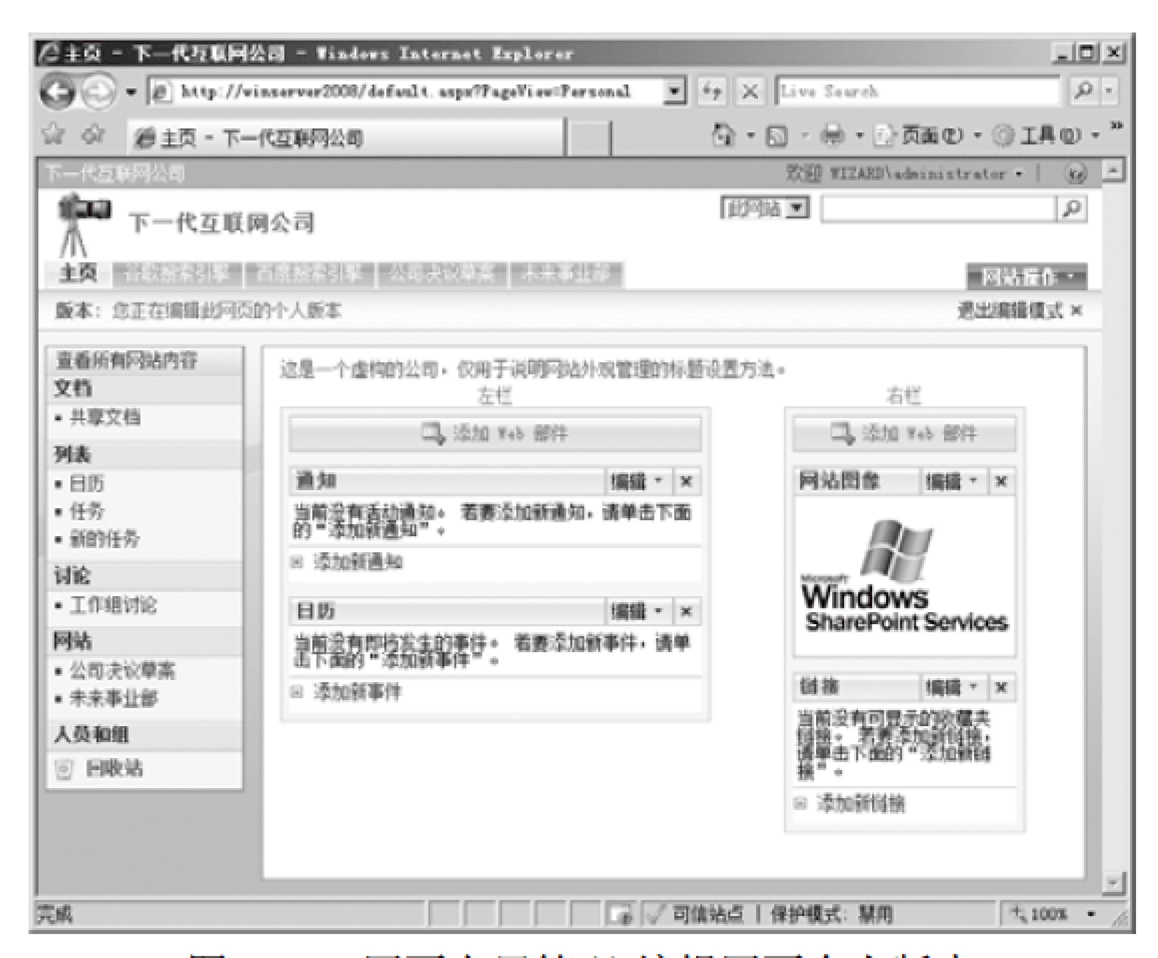


图 3-37　网页布局管理-编辑网页个人版本



图 3-38　网页布局管理-编辑网页共享版本

无论是编辑个人版本还是共享版本，在编辑网页时都可以根据需要改变当前页面上各个 Web 部件的相对位置(通过简单的拖拽即可实现)，也可以增加新的 Web 部件、设置 Web 部件的属性或删除现有的 Web 部件。在增添 Web 部件时，用户需要通过“添加 Web 部件”的网页对话框来选择一个或多个 Web 部件，以添加到页面中，如图 3-39 所示。



图 3-39　网页布局管理-添加 Web 部件

3.2.6　通知管理

通知功能使用户能够非常方便地在 WSS 网站发布各种通知信息。若要添加通知，用户只需登录到 WSS 网站，然后在主页上单击“添加新通知”链接即可。添加通知不要求用户有任何网页制作技术，只需像发送邮件一样确定通知的标题和正文，以及到期日期(用以设定该通知自动删除的日期)，如有需要，还可以添加“附加文件”，如图 3-40 所示。通知内容填写完毕后，单击“确定”按钮即可发布通知。

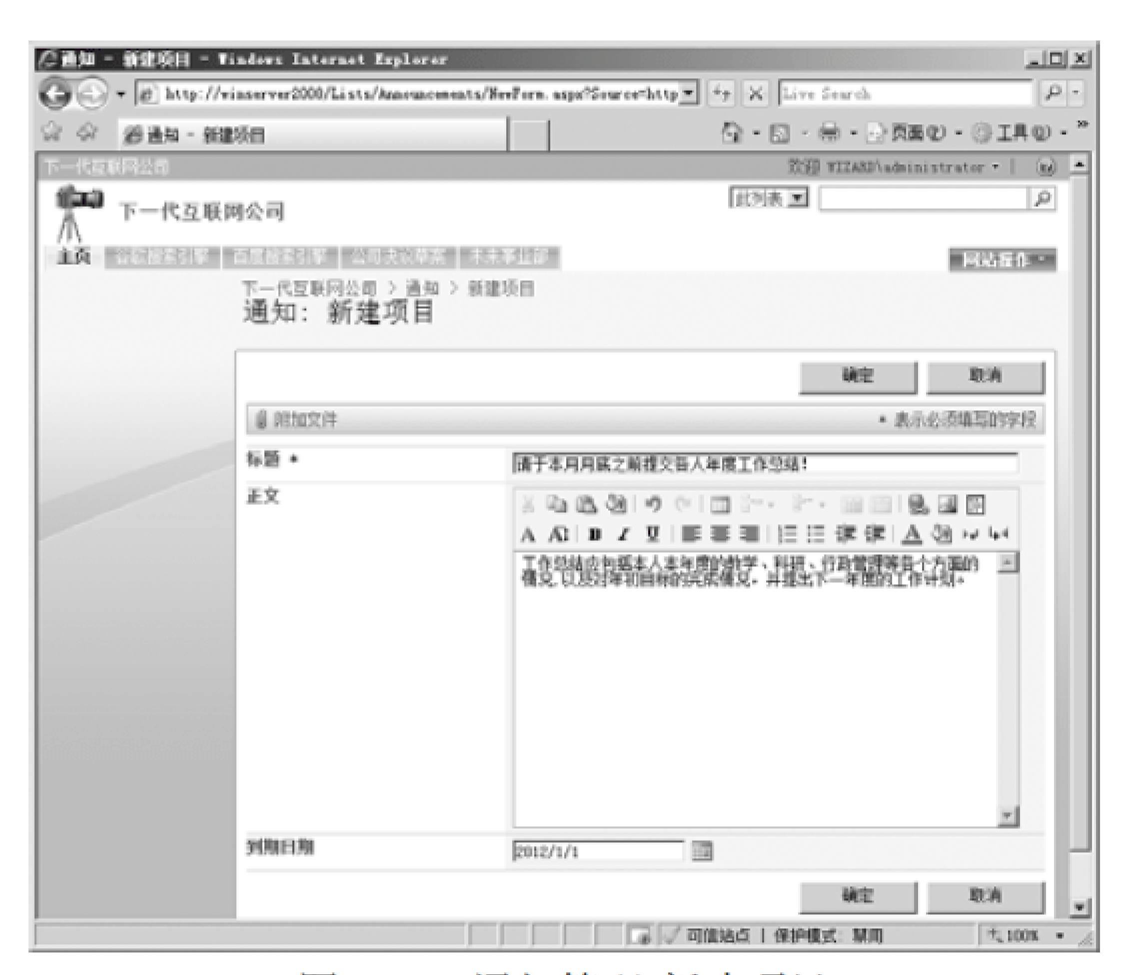


图 3-40　通知管理-新建项目

发布通知后，其他用户登录到 WSS 网站时，就会在主页上直接看到这条新的通知，如图 3-41 所示。如果发现通知内容有误，或者需要进一步修改，还可以重新编辑通知。只需在主页上单击相应的通知链接，即可进入查看通知页面，如图 3-42 所示。在此页面上，用户可以通过“编辑项目”链接重新编辑通知，也可以通过“删除项目”链接将该通知删去，还可以通过“管理权限”链接控制不同级别的用户或用户组针对该通知所拥有的权限。

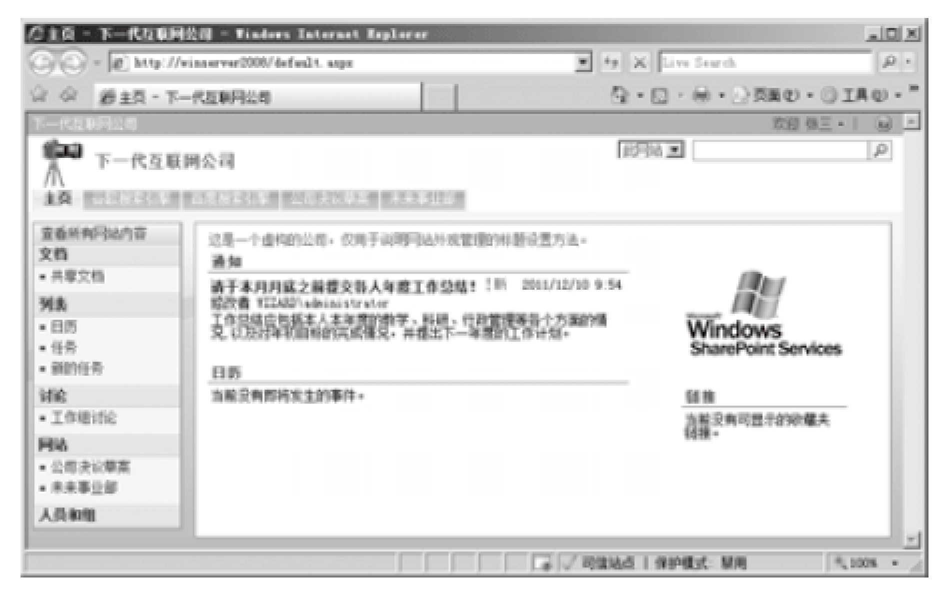



图 3-41　通知管理-主页上的通知消息



图 3-42　通知管理-查看通知页面

在查看通知页面中，用户还可以通过“通知我”链接新建一个以电子邮件进行通知的服务，如图 3-43 所示。建立了这种服务以后，WSS 会自动跟踪指定的项目、文档、列表或库的内容，并在其发生更改时自动发送电子邮件通知用户。此项邮件通知功能不仅可以在通知中使用，也可以在日历、任务等项目中使用。需要注意的是，要在 WSS 网站上启用该功能，必须先在服务器或虚拟服务器级别上配置并启用电子邮件服务器。



图 3-43　通知管理-新建邮件通知

3.2.7　日历管理

日历可以帮助用户管理与特定日期相关的各种项目，如即将举行的会议、时间期限和

法定节假日等。通过在日历中添加相应的事件，用户可以规划、跟踪需要在特定日期或时间段完成的工作。

如图 3-44 所示的是一个用户的日历页面。在此页面中，用户可以审阅当前日历中所包含的各个项目。如需增加新的项目，只需选择“新建”菜单中的“新建项目”命令，即可进入“日历—新建项目”页面，如图 3-45 所示。在此页面中，用户可以指定新建项目的标题、所在地点及起止时间，并根据需要加入项目说明。如有必要，还可以将项目指定为“全天活动”，或者设定项目的重复方式，如图 3-46 所示。如果项目是一次会议，则在新建该项目的时候，还可以选择使用“会议工作区”，以方便用户将来更好地组织与此事件相关的与会者、议程、文档、纪要和其他各种相关信息。

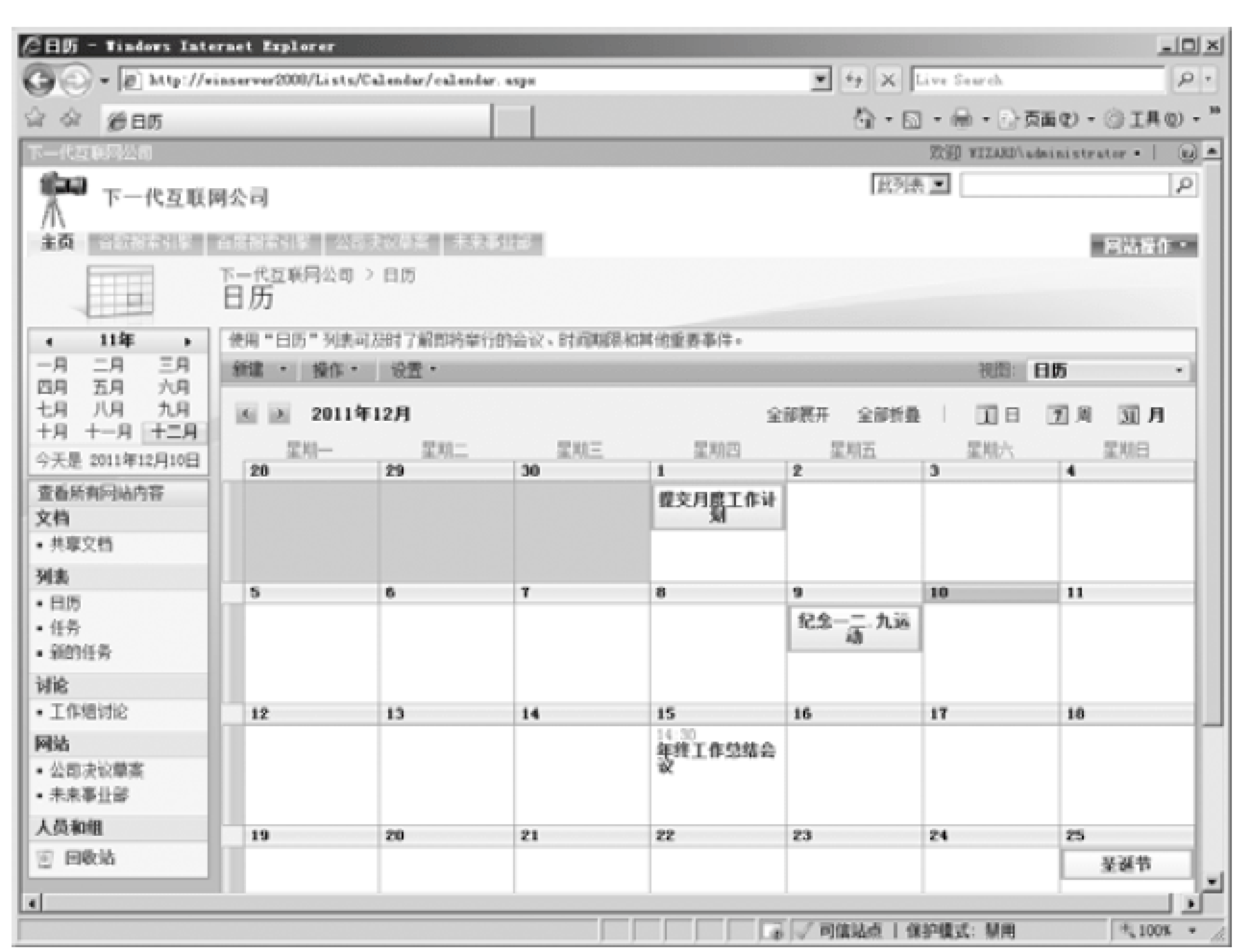


图 3-44　日历管理-日历界面



图 3-45　日历管理-新建项目



图 3-46　日历管理-设定重复

项目添加完毕后，即可显示在日历的相应日期位置。如需修改或删除某个项目，只需在日历中单击项目链接，进入项目相关页面(如图 3-47 所示)后，单击“编辑项目”链接或“删除项目”链接。需要注意的是，对于重复项目，采用上述方法只能删除选定日期的这一次项目。若要删除整个重复项目，需要单击重复项目相关页面上的“编辑序列”链接，然后在“编辑序列”页面中选择“删除项目”。



图 3-47　日历管理-编辑或删除项目

3.2.8　任务管理

“任务”列表可以用来跟踪用户或用户组需要完成的工作。通过“任务”列表，用户可以随时查看自己目前需要完成的任务标题、任务所分配的对象、任务的进行状态、进度和截止日期等信息，并可以根据需要随时更新相关的内容，以使其他用户随时了解任务状况。

默认情况下，“任务”列表的具体内容并不会出现在 WSS 站点的主页上。用户可以通过编辑网页的方式将“任务”所对应的 Web 部件添加到网页中以便查看，或者通过主页左侧的“任务”链接切换到“任务”列表页面，如图 3-48 所示。



图 3-48　任务管理-任务列表

如果要新建任务，可以通过单击“任务”列表页面中的“新建”按钮，在弹出的下拉菜单中选择“新建项目”，即可切换至“任务：新建项目”页面，如图 3-49 所示。在此页面中，用户可以设置任务的标题、优先级、状态、完成百分比、分配对象、说明信息和起止时间等内容，如有必要，还可以添加与任务相关的文件。

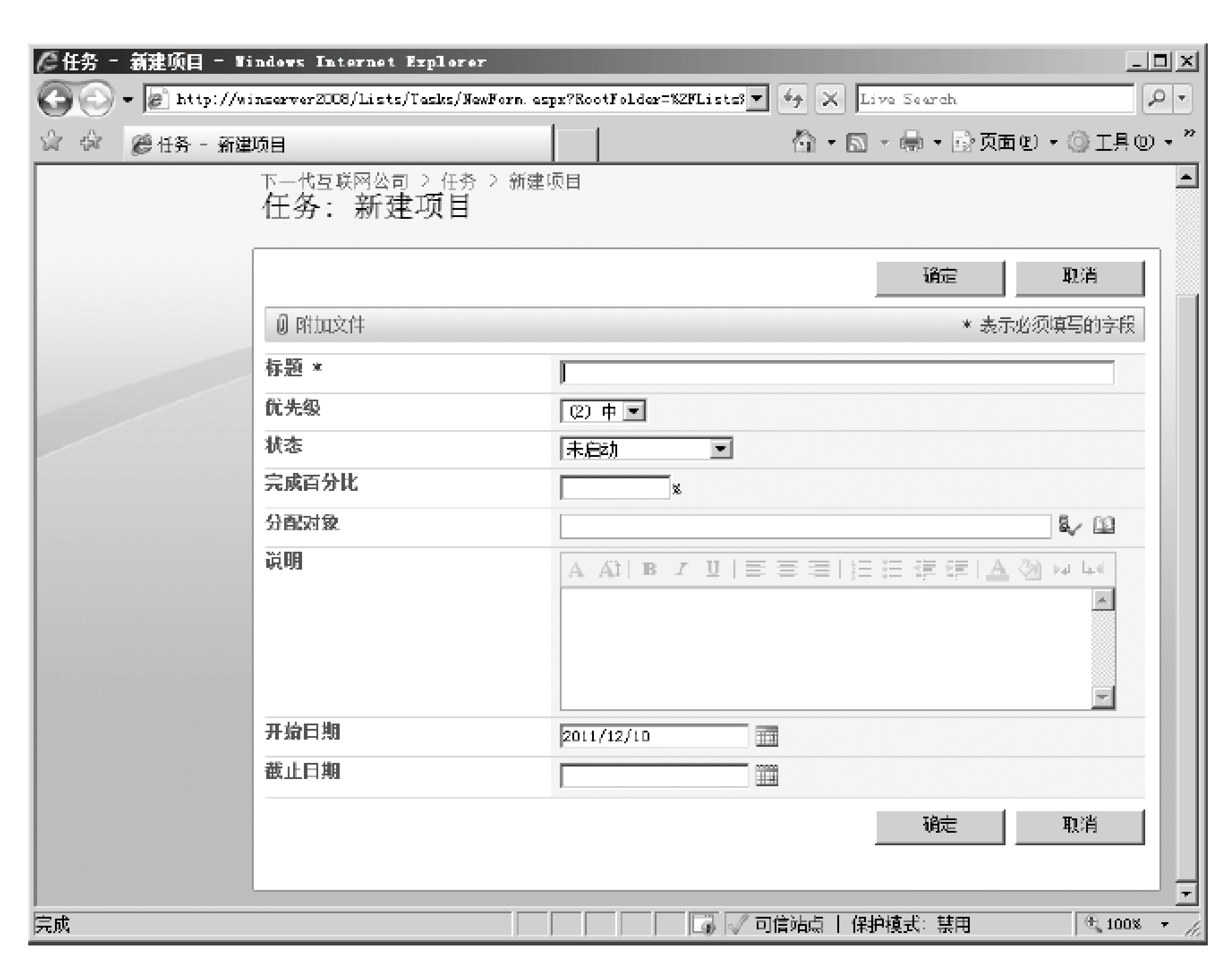


图 3-49　任务管理-新建项目

任务添加完毕后，还可以根据需要进行修改或是删除。只需在“任务”列表页面中选择相应的任务，单击任务标题右侧的箭头，在弹出的下拉菜单中选择“编辑项目”或“删除项目”即可，如图 3-50 所示；也可以通过单击任务标题切换到任务具体信息页面，如图

3-51 所示，然后再单击“编辑项目”按钮或“删除项目”按钮即可。

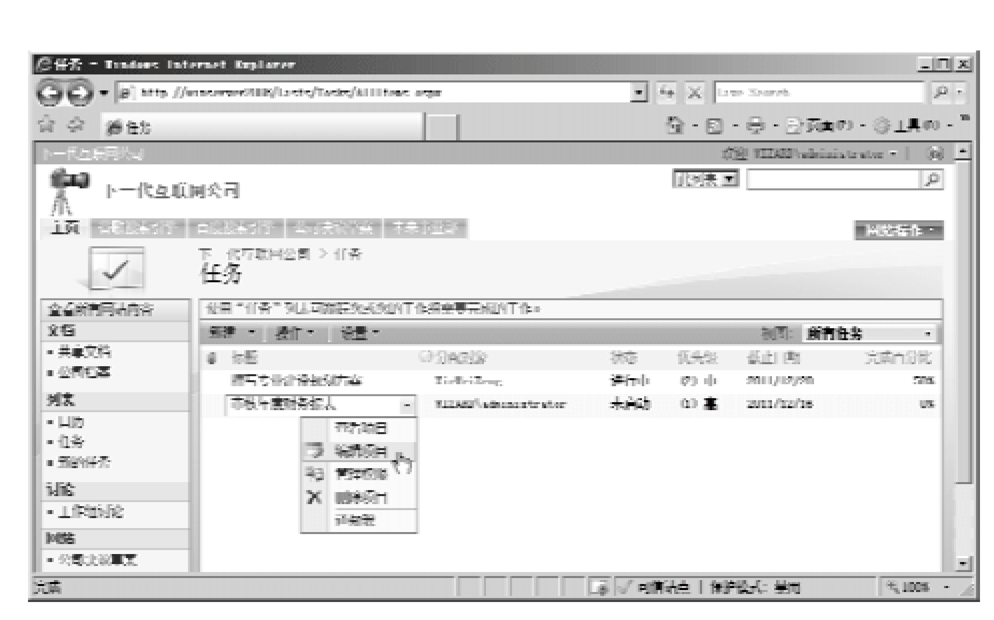


图 3-50　任务管理-编辑或删除项目



图 3-51　任务管理-任务具体信息

3.2.9　链接管理

除了 WSS 站点本身以外，用户还需要经常访问其他的站点，为了方便用户的访问，管理员可以把这些站点的地址链接加入到 WSS 站点的首页当中。要添加新的链接，只需在 WSS 站点主页上单击“添加新链接”链接即可。注意，没有相应权限的用户主页上是不会出现该链接的。如图 3-52 所示的就是新建链接项目的页面。在此页面中，管理员可以指定链接的 URL 地址、链接的说明及注释信息。单击“确定”按钮即可建立一个新的链接。如图 3-53 所示的是建立若干链接以后的 WSS 站点主页。



图 3-52　链接管理-新建链接



图 3-53　链接管理-添加链接的效果

链接添加完毕后，还可以随时根据需要进行修改或删除。管理员只需单击 WSS 站点主页上的名为“链接”的链接，即可切换到“链接”列表页面进行管理，如图 3-54 所示。管理员在相应链接的 URL 地址上单击一下，即可在弹出的快捷菜单中选择“编辑项目”或“删除项目”来实现修改链接或删除链接。



图 3-54　链接管理-链接基本操作

除此以外，管理员还可以通过“链接”列表页面中的“操作”按钮的各下拉菜单项实现以数据表格式批量编辑链接项目、更改链接项目的顺序或将链接列表导出到电子表格等操作，如图 3-55 所示。



图 3-55　链接管理-链接高级操作

3.2.10　文档库管理

用来存储、共享和编辑文件的库是 WSS 最主要的功能之一。WSS 3.0 支持以下 4 种类型的库。

- 文档库：当需要共享文档或其他文件集合时，可以创建文档库。文档库支持文件夹、版本控制和签出等功能。

● 表单库：当需要管理基于 XML 的业务表单时，可以创建表单库。
● Wiki 网页库：当需要拥有相互连接的 Wiki 网页集时，可以创建 Wiki 网页库。Wiki 网页库支持图片、表格、超链接和 Wiki 链接。
● 图片库：当需要共享图片时，可以创建图片库。图片库可以提供特殊的图片管理和显示，例如缩略图、下载选项和幻灯片放映。

一个 SharePoint 站点可以包含若干的文档、表单、图片和 Wiki 网页库。一般情况下，文档库是最基本、最重要也是使用最广泛的库类型。WSS 3.0 文档库提供了强大的 Web 内容管理功能，可以用于替换现存的文档共享方案。WSS 3.0 文档库可以实现以下功能：

● 为所有文档提供项目级别的安全。
● 使用 SharePoint 内置的工作流功能将业务流程附加到文档中。
● 为文档及其内容提供强大的版本控制。
● 为部门和项目组提供一个基于 Web 的、简单的组织文件的方法。
● 当文件被修改、升级、添加附件或删除时通知用户。
● 以灵活、可定制的视图显示每个文档库中的内容。
● 为管理文档的主要和次要版本提供内容审批功能。

默认情况下，WSS 站点会创建一个名为“共享文档”的文档库，用以存放需要与工作组成员共享的文档。当然，在 WSS 站点中也可以根据需要由管理员创建新的文档库。具体步骤如下：

(1) 以管理员身份登录 WSS 站点，在主页上单击“网站操作”按钮，在弹出的下拉菜单中选择“创建”命令，如图 3-56 所示。

(2) 在接下来的“创建”页面中单击“文档库”链接，以开始创建新的文档库，如图 3-57 所示。



图 3-56　文档库管理-创建



图 3-57　文档库管理-新建文档库

(3) 在随后的“新建”页面中输入新文档库的名称、说明信息，指定是否在“快速启动”栏上显示该文档库，以及是否在每次编辑此文档库的文件时创建版本，最后指定此文档库中新文件所采用的文档模板，如图 3-58 所示。单击“创建”按钮，即可建立新的文档库。



图 3-58　文档库管理-输入文档库参数

新建立的文档库是空的，不包括任何文档。用户可以通过文档库页面上的“新建”菜单中的“新建文档”命令直接在库中创建新文档，如图 3-59 所示，也可以通过“上载”菜单中的“上载单个文档”命令将某个现有文档添加到文档库中。

添加文档后，即可在文档库页面上查看该文档的类型、名称、修改时间及修改者等信息。如需对文档做进一步操作，可以在文档名称上单击，然后在弹出的菜单中选择相应的命令，如图 3-60 所示。下面列出了各个命令所对应的功能。





图 3-59　文档库管理-新建文档



图 3-60　文档库管理-文档的进一步操作

- 查看属性：显示一个列出文档所有可用属性描述信息的 Web 页，里面也包含可用的选项，即编辑、删除、管理权限、管理副本、签出、版本历史记录、通知我。这个页面也显示不同用户创建和最后修改的日期和时间，如图 3-61 所示。
- 编辑属性：显示一个用来修改当前文件信息的 Web 页，也可以选择删除项目。这个页面还显示了文档的修订版本及创建和每次修改所涉及的用户、日期和时间。
- 管理权限：显示一个可以管理文件权限的 Web 页。页面说明描述了文档的继承状态。管理员可以管理继承的权限或者编辑权限，如果编辑权限，继承的权限将取消，这时可以为这个对象设置独立的权限。
- 在(适当的 Office 程序)中编辑：启动适当的 Office 应用程序，并打开当前的文档。根据文档类型，默认打开文件的应用程序会相应变化。如果文件的扩展名是.docx，

那么选项则是“在 Microsoft Office Word 中编辑”。

- 删除：这个选项可以把当前文档从文档库中删除。
- 发送到：让用户可以把文件发送到其他位置或者执行附加的操作。“发送到”的子选项包括“其他位置”、“通过电子邮件发送链接”、“创建文档工作区”和“下载副本”。
- 签出：锁定文档库中的文档拷贝，除了签出这个文件的人，没有人可以修改这个文件。当签出生效以后，“签入”命令将会出现在这个位置。
- 版本历史记录：如果文档库打开了文档历史记录功能，这个选项会显示出所有的列表。这个列表包含历史记录数量、最后修改时间、相关人员、文档大小以及相关的注释，如图 3-62 所示。管理员可以删除所有历史记录，删除草稿历史记录，或恢复以前的历史记录。
- 通知我：在“通知我”页面上可以决定文档发生变化的通知邮件的发送对象，以及邮件的发送频度。



图 3-61　文档库管理-查看属性



图 3-62　文档库管理-文档版本历史记录

通常文档都是事先由用户创建好的，然后登录到 WSS 站点进行上传。事实上，Word 内置了文档发布功能，允许用户在文档编辑完成后，直接上传到 WSS 网站并创建一个文档工作区，而不必登录到 WSS 站点去上传(需要用户修改系统 Internet 属性，预先将 WSS 站点地址添加到可信站点区域)。以 Word 2007 为例，具体操作步骤如下：

(1) 在完成文档编辑操作后，激活 Word 的主菜单，选择“发布”菜单中的“创建文档工作区”项命令，如图 3-63 所示。

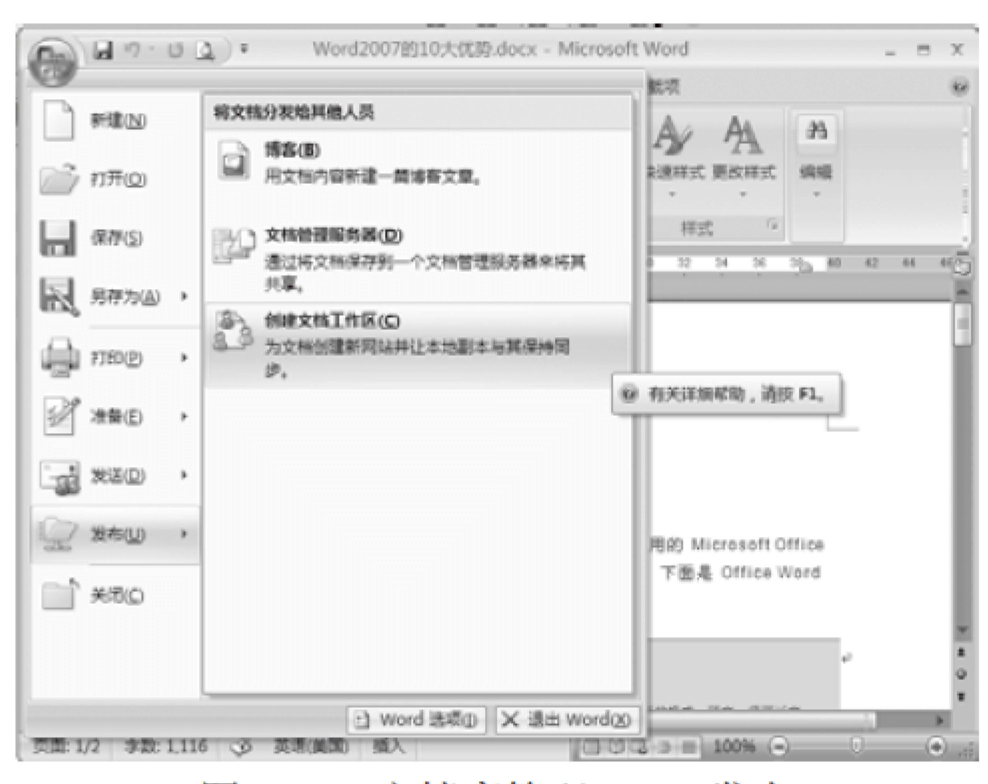


图 3-63　文档库管理-Word 发布

(2) 在“文档管理”侧边栏中输入文档工作区的名称(默认为该文档的名称)和新工作区所在的位置(即 WSS 站点地址)，如图 3-64 所示。



图 3-64　文档库管理-Word 发布-工作区位置

(3) 单击“创建”按钮后，Word 即可开始新建文档工作区，如图 3-65 所示。因此时需要访问 WSS 站点，所以如果当前计算机还没有加入域，则会显示要求输入用户名和密码的登录文本框；如果已经加入域并以域用户身份登录，则不会出现登录文本框。



图 3-65　文档库管理-Word 发布-正在新建工作区

文档发布成功后，即可在“文档管理”侧边栏中显示当前文档状态、文档工作区的成员、任务及所包含的文档和链接等信息，如图 3-66 所示。单击侧边栏上部的链接“在浏览器中打开网站”，即可在浏览器中以相应用户身份登录 WSS 站点，并打开刚刚创建的文档工作区，如图 3-67 所示。



图 3-66　文档库管理-Word 发布-发布成功



图 3-67　文档库管理-Word 发布-浏览器查看

同样，Excel 和 PowerPoint 也都内置了文档发布功能，在编辑完成电子表格或演示文稿以后，都可以通过文档发布功能直接将文档上传到 WSS 网站并创建文档工作区。因操作步骤与 Word 雷同，在此不再赘述。

3.3　使用 WSS 模板

3.3.1　WSS 模板功能介绍

WSS 模板是围绕特定业务需求设计的预建定义。用户可以按原样使用这些模板来创建属于自己的 SharePoint 网站，然后再根据需要自定义该网站。WSS 提供的默认网站模板主要有以下几种。

- 工作组网站：用来快速组织、编写和共享信息。它提供了文档库和列表来管理通知、日志项、任务和讨论板。
- 空白网站：个人按照自己的需求定制的空白网站。
- 文档工作区：团队用来协同完成一个文档的网站。它提供一个用来存储主要文档和支持文件的文档库、一个分配任务的任务列表和一个相关文档资源的链接列表。
- Wiki 网站：团队用来头脑风暴和共享观点的网站。它提供了可以快速编辑记录信息，并且能通过关键词连接的页面。
- 博客：个人或者团队用来发表观点、观察报告和专业观点的网站，而浏览者可以在上面批注。
- 基本会议工作区：用来计划、组织会议，并在会后总结的网站。它提供了管理议程、会议议题和文档等一系列的列表。
- 空会议工作区：个人用来按照需求定制的空白会议网站。
- 决议会议工作区：用来跟踪会议状态或达成决议的网站。它提供了创建任务、存储

文档和记录决议等列表。

- 社会活动工作区：用来规划社会活动的网站。它提供跟踪议题、准备指导和存储活动图片的列表。
- 多页会议工作区：用于规划、组织和获取会议结果的网站。它提供了可以管理议程和会议议题的列表，以及两个可以根据需求定制的空白页面。

这些模板非常适合公司环境中的信息工作者。多数人会使用这些模板来创建网站，同时这个平台也可以用来定制开发各种各样的应用程序。这些模板可以帮助用户灵活地完成文档、会议、事件、项目、讨论和观点上的协作。对于需要对文档保留版本、管理讨论，以及跟踪任务、问题和议题的部门或者项目成员来说，这些模板也是非常有用的。通过采用这些新技术，用户可以在安全和可控的环境中，使文档内容保持最新。

除了提供默认模板以外，WSS 还允许用户将自己的网站快速保存为模板。当一个 SharePoint 用户完成对网站的修改和构建之后，网站及其内容就可以被保存为一个模板。拥有权限的其他人可以根据此模板创建一个新的内容相同、布局相同、导航相同的网站，这个功能适合那些想要创建多个外观相同网站的组织。这样做可以比手工定制网站节约几个小时乃至几天的时间。

将 SharePoint 网站另存为模板时，保存的是该网站的总体框架，包括该网站的列表和库、视图、窗体以及工作流。除了这些组件外，如果用户在保存模板文件时选择“包含网站内容”，则在模板中还会包括该网站的具体内容，例如存储在文档库中的文档。

要将当前网站保存为模板，只需以管理员身份登录 WSS 网站，单击主页上的“网站操作”按钮，在弹出的下拉菜单中选择“网站设置”，进入“网站设置”页面，如图 3-68 所示，单击“外观”类别下的“将网站另存为模板”链接，在“网站另存为模板”页面中输入要保存的模板文件的文件名、模板名称和说明信息，如图 3-69 所示，再选定是否包含网站内容，然后单击“确定”按钮，即可创建新的模板，如图 3-70 所示。新的模板会自动保存到网站模板库中，如图 3-71 所示，以后用户就可以基于该模板创建网站了。



图 3-68　WSS 模板-网站设置



图 3-69　WSS 模板-网站另存为模板



图 3-70　WSS 模板-模板创建成功

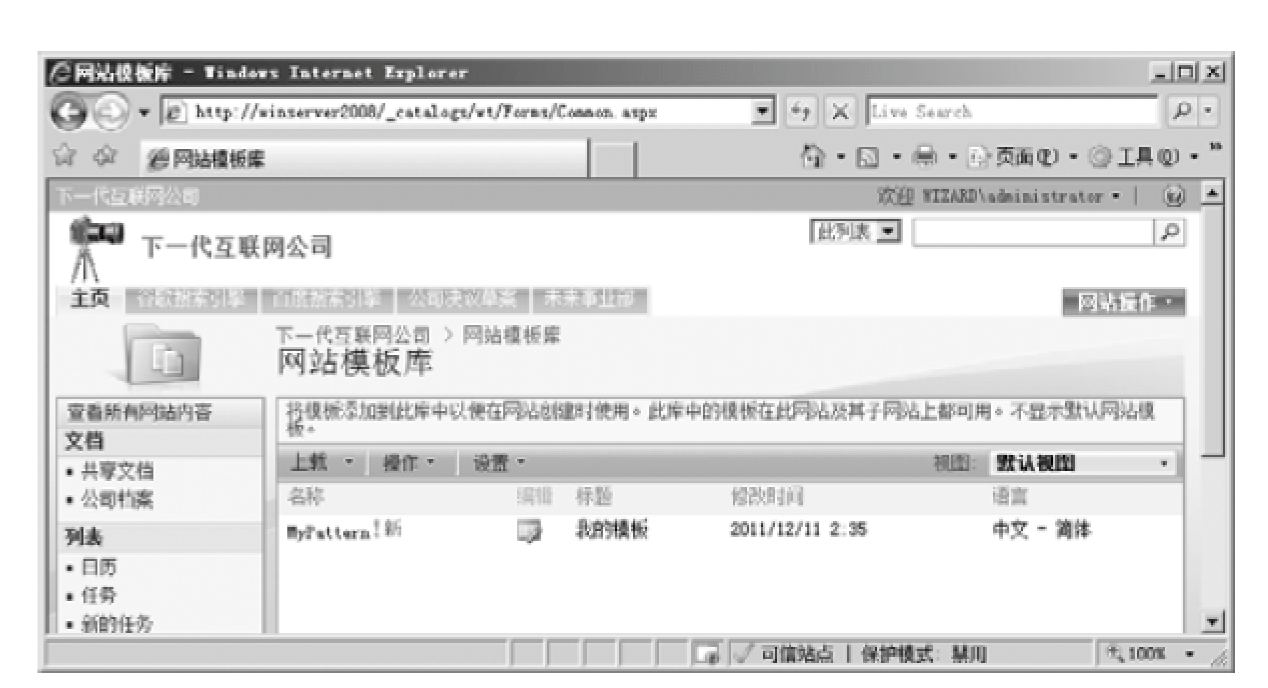


图 3-71　WSS 模板-网站模板库

3.3.2　将模板上载到 WSS 网站

要将保存好的模板文件应用到某个 WSS 网站，必须先将其上载到 WSS 网站中。操作步骤如下：

(1) 以管理员身份登录 WSS 网站，单击主页上的“网站操作”按钮，在弹出的下拉菜

单中选择“网站设置”，进入“网站设置”页面。

(2) 单击“库”类别下的“网站模板”链接，在“网站模板库”页面中的单击“上载”按钮，选择“上载单个文档”命令，如图 3-72 所示。



图 3-72　WSS 模板-网站模板库-准备上载文档

(3) 在接下来的“上载模板”页面中输入模板文件的路径和名称，如图 3-73 所示，单击“确定”按钮，即可完成模板上载的过程。

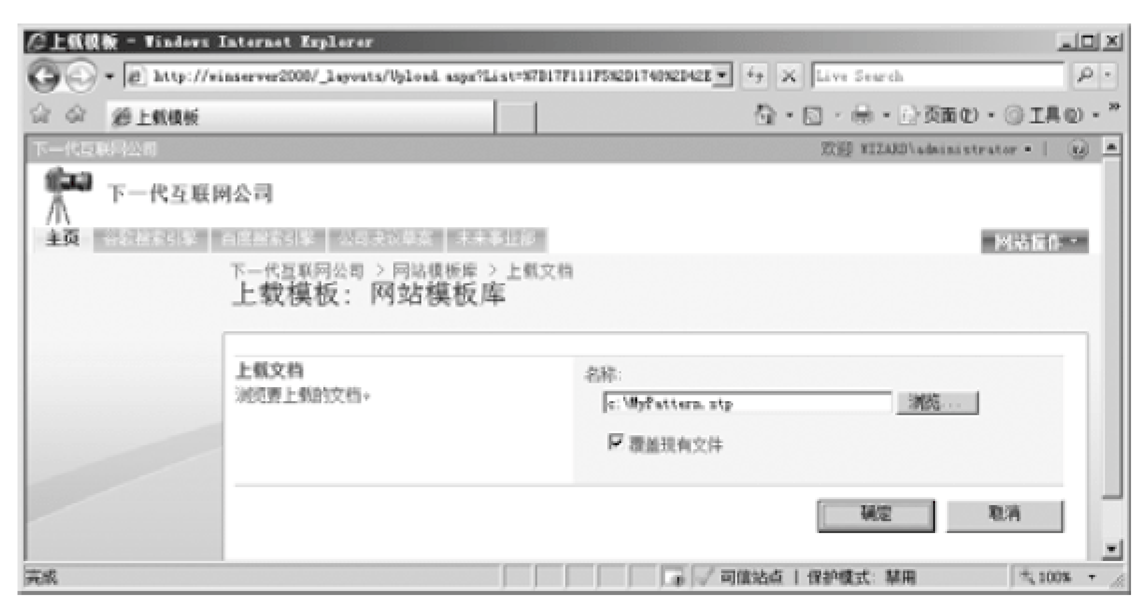


图 3-73　WSS 模板-网站模板库-上载模板文档

模板上载到 WSS 网站以后就会出现在网站模板库中。当管理员需要使用该模板创建新的网站时，只需在“新建 SharePoint 网站”页面中输入新建网站的标题和说明信息，并在“选择模板”位置切换到“自定义”选项卡，然后在模板列表中选择上载过的自定义模板就可以了，如图 3-74 所示。



图 3-74　WSS 模板-使用模板新建网站

3.4　本章小结

WSS 为创建 SharePoint 站点提供了丰富的列表样式，灵活的文件存储，并允许用户对列表字段进行扩展，而且权限分配也很方便，使得用户能在文档、任务、联系人、事件以及其他信息上开展协作。这些站点将文件存储带入到了一个新的水平，为团队协作提供了一个活动空间，它使基于文档、任务和活动的协作成为可能，并且使得共享联系人和其他信息的过程变得更为轻松。WSS 允许团队和站点的管理人员更容易地管理站点内容和用户活动，使用可靠的管理控件来管理存储和 Web 基础架构，实现和管理高性能协作环境，从而提高业务流程的效率。

WSS 不仅能够创建用于信息共享和文档协作的 SharePoint 站点，还可以与日常工具(如 Microsoft Office 系列或第三方平台)紧密集成并协同工作，通过采用基于 Web 的界面方便用户使用，还可以消除冗余解决方案的成本支出，达到快速部署、简化管理，改善工作流程，降低成本的目的。

WSS 所提供的协作功能能够使工作组方便地访问所需的人员、文档和信息，以便用户在工作中做出更合理的决策，从而帮助工作组保持沟通顺畅并提高工作效率；门户功能对于设计、部署和管理企业 Intranet 门户、公司 Internet 展示网站和部门门户网站都非常有用；搜索功能可以使用户不仅能够对 WSS 中的文档、页面、和数据进行搜索，还能搜索到企业中其他站点、文件共享目录，并且 WSS 的搜索是支持权限过滤的；企业内容管理功能提供了文档管理、记录管理、表单管理、web 内容管理等服务；表单驱动功能将基于 XML 的简单易用的智能电子表单与现有的系统无缝集成，简化了表单驱动的业务过程。

3.5　思考与练习

【思考题】

1. 默认情况下，WSS 会生成哪 3 个 SharePoint 用户组？它们各有什么权限？
2. 对 WSS 网站的外观管理主要包括哪几个方面？
3. WSS 的文档库具备哪些功能？
4. 如何使用现有的 WSS 模板？如何创建新的 WSS 模板？

【练习题】

初始条件：一台尚未安装 Windows SharePoint Services 的 Windows Server 2008 服务器、服务器管理员帐户。

操作目标：在服务器上安装并启用 WSS 服务。

第4章　DNS服务

【本章导读】

网络中使用 IP 地址来标定一台服务器的身份，因此用户在共享网络服务的同时，需要知道服务器的 IP 地址，这就增加了网络访问的难度。为此，网络中又出现了一种新的标定服务器的方法：域名系统。DNS(Domain Name System，域名系统)服务，就用来记录 IP 地址和域名之间的对应关系，以方便用户查询，从而降低了使用网络服务的难度。Windows Server 2008 中提供了强大易用的 DNS 服务组件，可以方便地提供 DNS 服务器。同时 Windows 网络中的 DNS 服务配合微软特有的活动目录服务，提供了更加强大和灵活的网络服务，极大地扩展了企业网络的功能，提高了企业网络的性能。

4.1　DNS 服务概述

互联网中的计算机，无论是客户端还是服务器，都是用 IP 地址作为唯一的网络标识的。众所周知，IP 地址就是一个 32 位的二进制编码，也可以写成点分十进制形式，但无论是二进制还是十进制的写法，都非常难记忆，为此人们还用域名的形式来标明一个网站的服务器。但是，域名是不能够在网络中使用的，这就需要有一种能够帮助用户将域名和 IP 地址进行相互转换的服务，这就是域名解析服务，简称 DNS。

4.1.1　DNS 服务简介

在配置计算机的 IP 地址时，需要输入计算机的 IP 地址、子网掩码、默认网关和 DNS 地址。即使是家庭中的拨号、ADSL 等连接手段，不需要手工配置这些参数，计算机在联入 Internet 时也会从 ISP 的服务器上自动获取这些参数。下面以用户使用浏览器浏览网页为例来说明 DNS 的工作流程。

某用户的 IP 地址是 218.28.137.89，DNS 为 202.102.224.68，备用 DNS 为 202.102.227.68，现在该用户打开浏览器，在地址栏中输入微软公司的网址 www.microsoft.com，并按下回车键。此时浏览器开始尝试连接该网址。众所周知，网址是无法在网络上作为主机标志的，必须首先把网址转化为对应的 IP 地址才可以。浏览器会首先查询本地缓存，如果本地缓存中有对应的信息，则按照查找到的 IP 地址尝试连接网站服务器，如果在本地缓存中没有找到该网站对应的 IP 地址，则根据网络配置信息中的 DNS 地址，浏览器向 DNS 服务器发出查询申请。DNS 收到查询申请后，在自己的数据库中查找 www.microsoft.com 对应的 IP 地址，如果能够找到，则将查询结果发给浏览器，如果查询不到，则向其他 DNS 服务器发

出查询申请，直至查询成功或确认其他 DNS 服务器也没有记录相应信息为止。浏览器向 DNS 服务器发出查询申请后，如果一段时间后收不到 DNS 服务器发来的信息，则向备用 DNS 服务器发出相同的请求。如果浏览器可以从 DNS 服务器或者备用 DNS 服务器获取该网站对应的 IP 地址，则尝试连接该 IP 地址对应的服务器，如果以上方法都不能让浏览器获取到对应的 IP 地址，则给用户提示，表示无法解析地址。

DNS 工作流程图如图 4-1 所示。

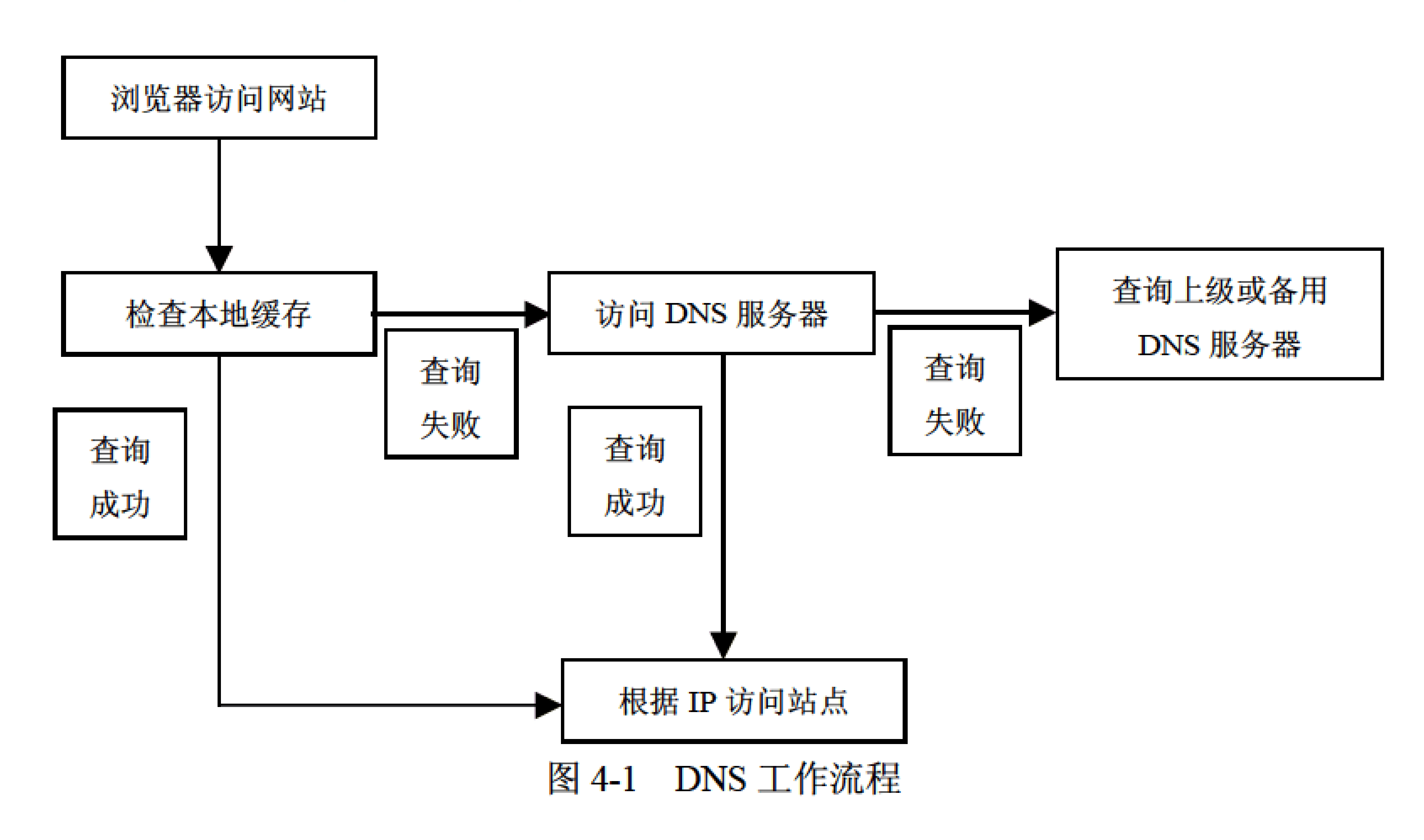


图 4-1　DNS 工作流程

4.1.2　查询模式

从查询内容上看，DNS 服务器有以下两种查询模式。

1. 正向查询

正向查询是指客户向 DNS 服务器发送一个域名，DNS 服务器经过查找，返回该域名对应的 IP 地址。

2. 逆向查询

逆向查询是指客户向 DNS 服务器发送一个 IP 地址，DNS 服务器经过查找，返回该 IP 地址对应的域名。

从查询方法上看，DNS 服务器也有以下两种查询方法。

1. 递归查询

用户需要查询某个域名对应的 IP 地址，但是当前的 DNS 服务器没有该记录，此时 DNS 服务器会替代用户向其他 DNS 服务器发出查询申请。递归查询常用于客户向 DNS 服务器申请服务。

2. 迭代查询

如果某 DNS 服务器接收到一个查询请求，但是它本身没有相关记录，则该 DNS 服务器会向其他 DNS 服务器提出查询申请，如果其他 DNS 服务器也没有相关记录，则会向第一台 DNS 服务器提供另一个 DNS 服务器的地址，以便 DNS 服务器继续查询。迭代查询一般用于 DNS 服务器之间的查询。

4.2　DNS 服务器的安装

Windows Server 2008 在默认状态下没有安装 DNS 服务，需要管理员手工添加。DNS 服务器需要固定的 IP 地址，因此作为 DNS 服务器的计算机不能通过自动分配的方式获取 IP 地址，必须手工配置。IP 地址设置完毕后，按照以下步骤安装 DNS 服务器。

(1) 以系统管理员帐户 Administrator 的身份登录到 Windows Server 2008 中，选择“开始”菜单→“管理工具”→“服务器管理器”命令，如图 4-2 所示。



图 4-2　“服务器管理器”界面

(2) 在服务器管理器界面的左侧选择“角色”，然后单击右侧窗口中的“添加角色”，打开角色添加向导，进入“选择服务器角色”界面，并单击“DNS 服务器”选项，如图 4-3 所示。

(3) 单击“下一步”按钮，进入“DNS 服务器简介”界面，如图 4-4 所示。



图 4-3　“选择服务器角色”界面



图 4-4　“DNS 服务器简介”界面

(4) 单击“下一步”按钮，进入“确认安装选择”界面，如图 4-5 所示。



图 4-5　“确认安装选择”界面

(5) 单击“安装”按钮，开始安装 DNS 服务器，如图 4-6 所示。



图 4-6　安装界面

(6) 等待几分钟后安装完毕，如图 4-7 所示。单击“关闭”按钮退出向导，DNS 服务器安装完毕。

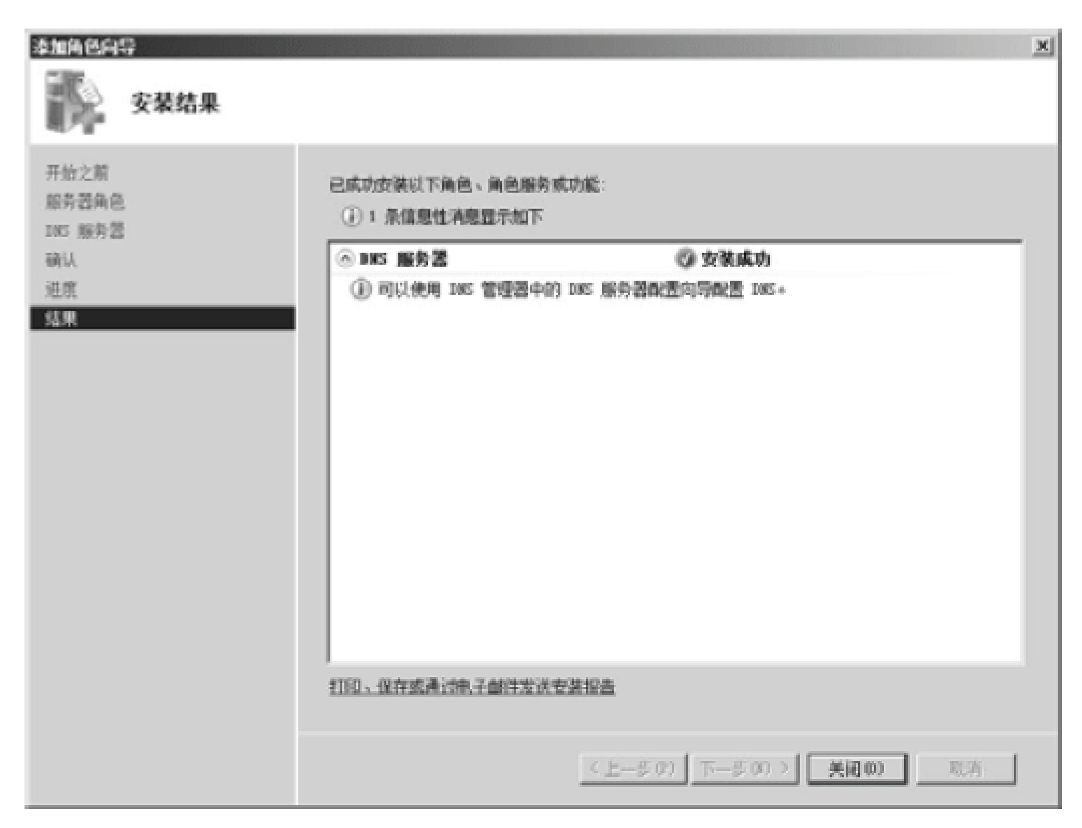


图 4-7　完成安装界面

4.3　DNS 服务器的配置与管理

DNS 服务器安装完毕后，系统不会自动启动配置向导，因此需要管理员手工配置 DNS 域、添加相应的正、反查找区域以及其他主机记录，将域名和 IP 地址一一对应起来，从而为用户提供域名解析服务。

4.3.1　添加正向搜索区域

为了使 DNS 服务器可以正常解析域名，必须先向 DNS 区域中添加正向查找区域。如果有需要，DNS 服务器允许管理员添加多个区域，以便解析多个域名。

(1) 选择“开始”菜单→“管理工具”→“DNS”命令，打开 DNS 管理器，展开左侧窗口的树形目录，单击“正向查找区域”，如图 4-8 所示。

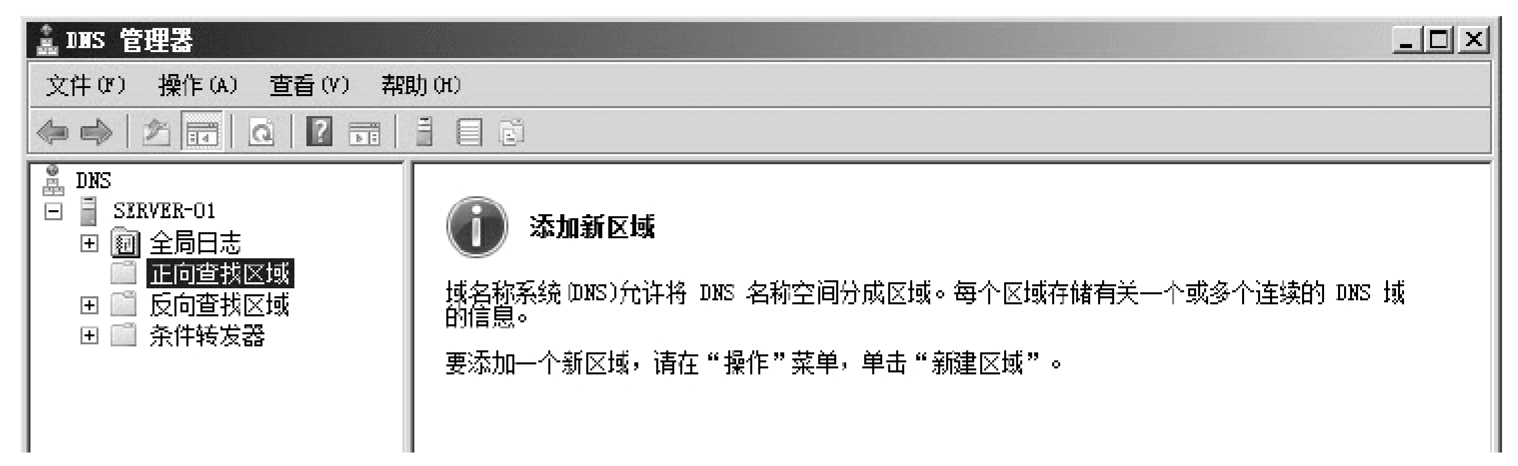


图 4-8　“DNS 管理器”界面

(2) 右击“正向查找区域”，在弹出的快捷菜单中选择“新建区域”命令，打开新建区域向导，如图 4-9 所示。

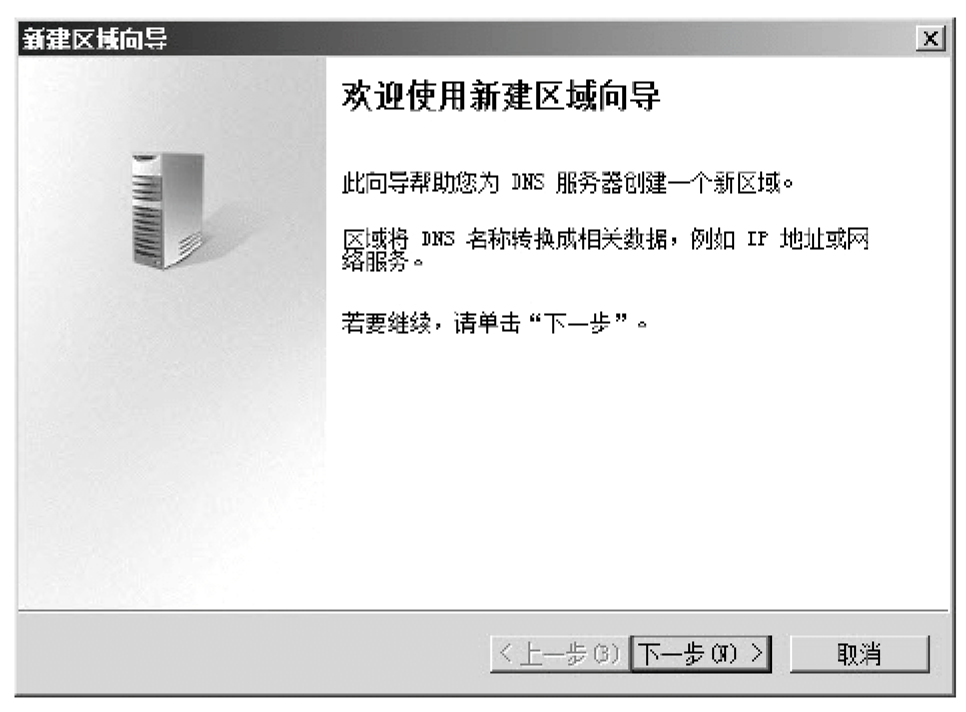


图 4-9　“欢迎使用新建区域向导”界面

(3) 单击“下一步”按钮，进入“区域类型”界面，如图 4-10 所示。本界面中有 3 种类型可供选择。如果要直接在当前服务器上创建 DNS 区域，则选择“主要区域”；如果 DNS 区域在其他服务器上创建，而当前服务器是作为辅助 DNS 服务器存在，则选择“辅助区域”；如果创建只含有名称服务器(NS)、起始授权机构(SOA)和粘连主机(A)记录的区域的副本，则选择“存根区域”。

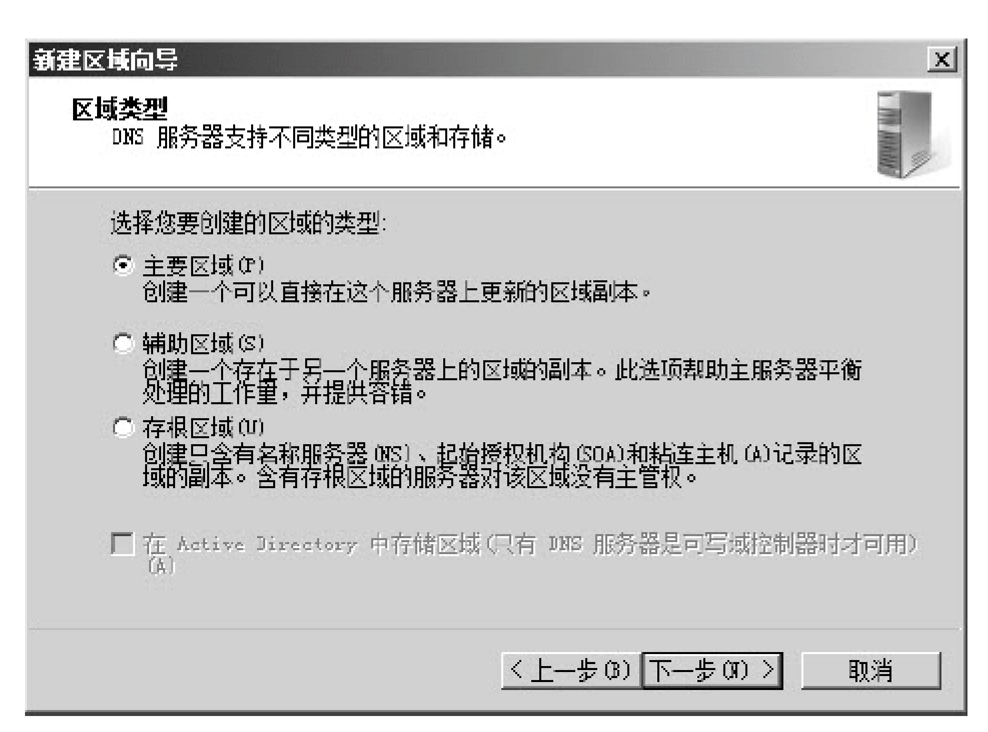


图 4-10　“区域类型”选择界面

(4) 本示例中选择“主要区域”，单击“下一步”按钮，进入“区域名称”界面，在“区域名称”文本框中输入在域名服务机构申请的正式域名，如 microsoft.com，如图 4-11 所示。区域名称用于说明 DNS 名称空间的部分，可以是域名或者子域名。

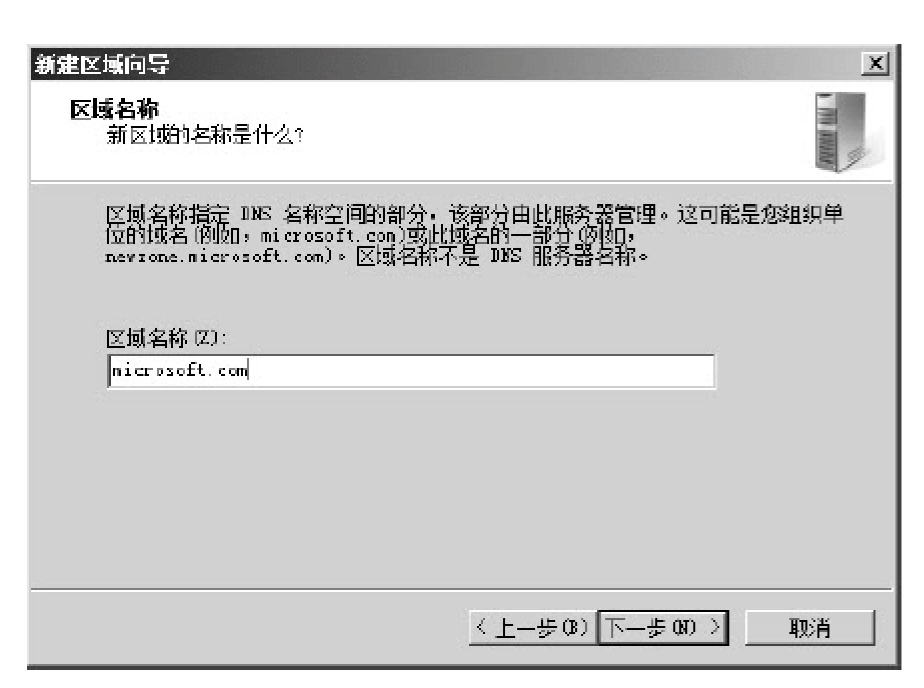


图 4-11　“区域名称”界面

(5) 单击“下一步”按钮，进入“区域文件”界面，如图 4-12 所示。选中“创建新文件，文件名为”单选按钮，在服务器上创建一个新的区域文件存储相关信息，文件名可以自定义，但是尽量使用默认值。如果要从另一个 DNS 服务器复制记录文件到当前服务器，则选中“使用此现存文件”单选按钮。

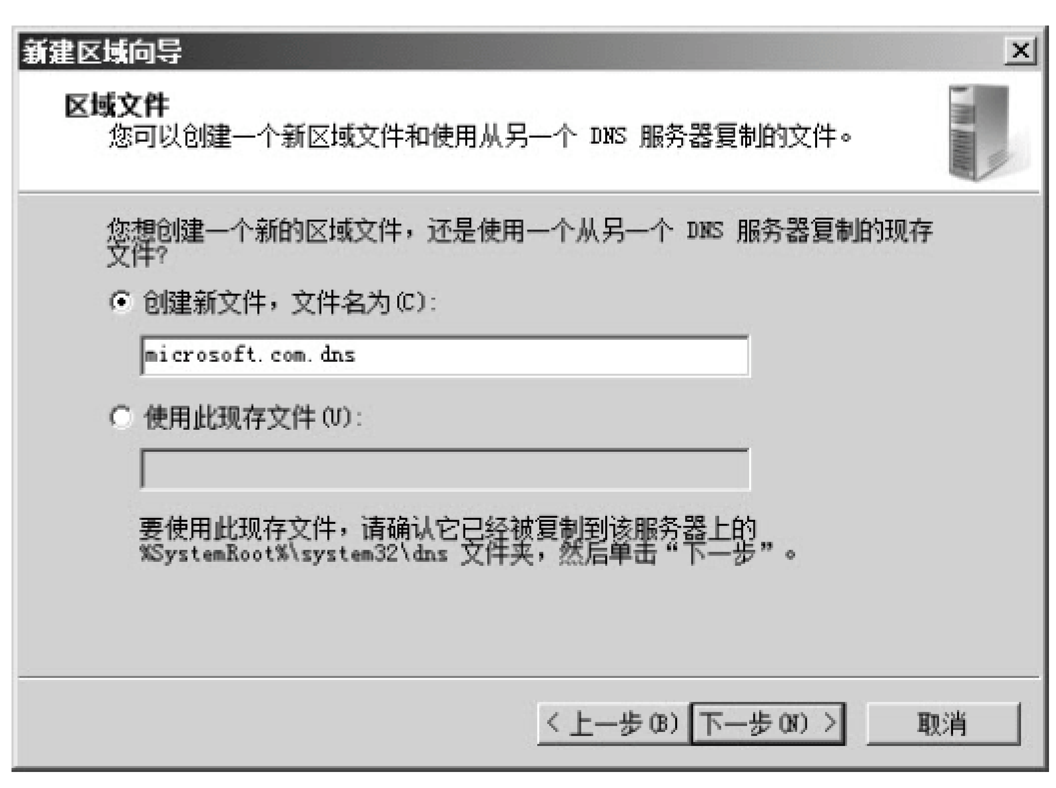


图 4-12　“区域文件”界面

(6) 单击“下一步”按钮，进入“动态更新”界面，选择动态更新方式，如图 4-13 所示。各选项含义如下。

- 只允许安全的动态更新(适合 Active Directory 使用)：如果当前 DNS 服务器用于活动目录的作用区域，才能使用该选项；
- 允许非安全和安全动态更新：该选项可以使任何客户端都接受资源记录的动态更新，对于使用 DHCP 功能获取网络地址的客户较为方便，但是由于也可以接受来自非信任源的更新，所以安全性较差；
- 不允许动态更新：可以使此区域不接受资源记录的动态更新，安全性较高，建议选择该选项。

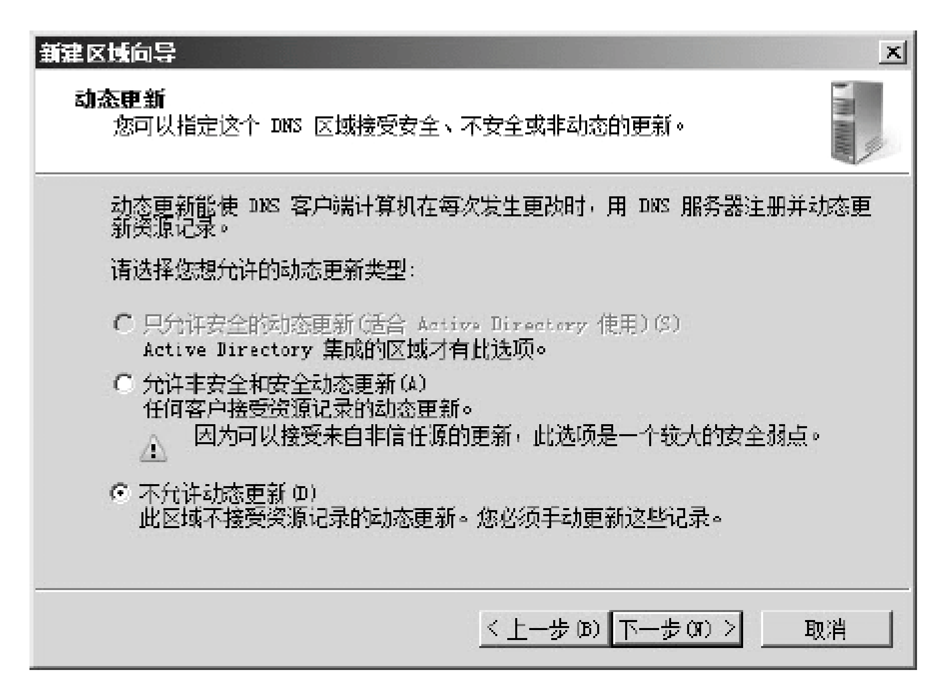


图 4-13　“动态更新”界面

(7) 这里选择“不允许动态更新”，单击“下一步”按钮，进入“正在完成新建区域向导”界面，如图 4-14 所示。如果还需要对前面的设置做修改，可单击“上一步”按钮返回并修改设置。

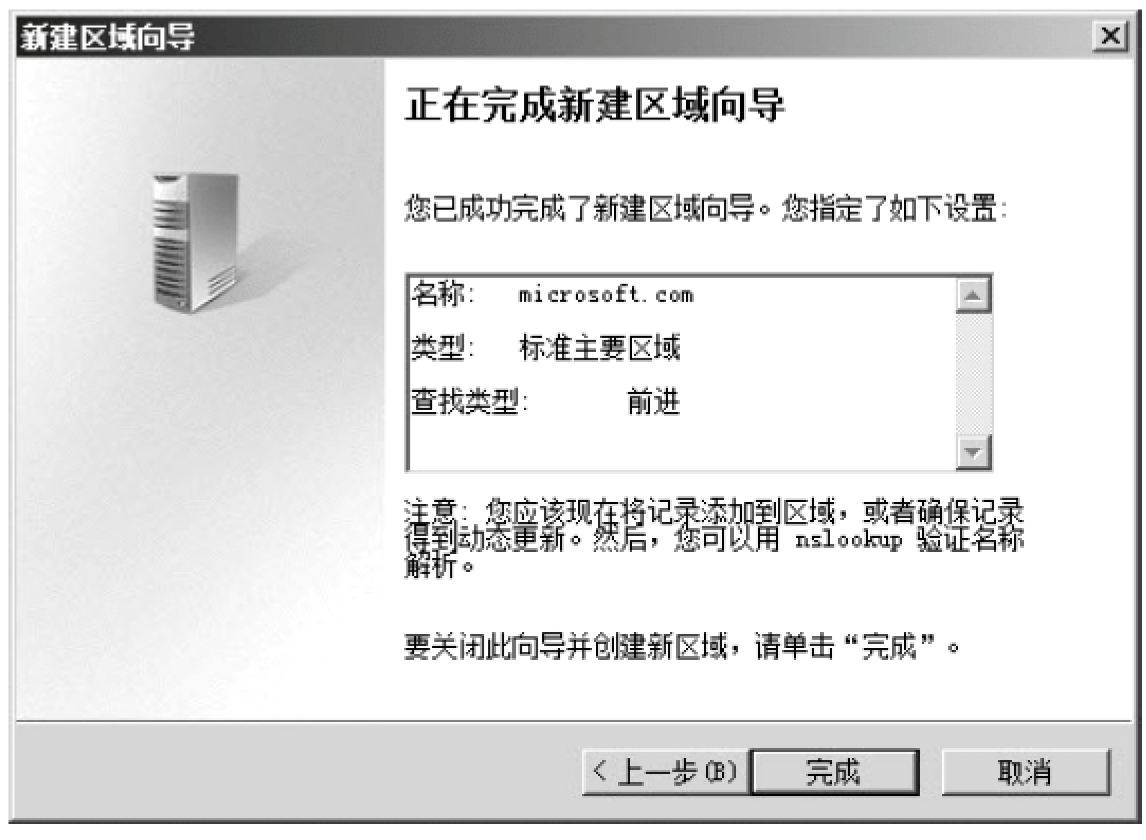


图 4-14　“正在完成新建区域向导”界面

(8) 如果不需要更改设置，单击“完成”按钮返回 DNS 管理器，此时新建的区域已经出现在 DNS 管理器中，如图 4-15 所示。



图 4-15　“DNS 管理器”窗口

至此已经完成了一个区域的添加，利用以上方法，可以添加多个 DNS 区域，分别指定不同的域名称，从而可以解析多个名。

4.3.2　添加 DNS 域

DNS 区域是 DNS 服务的基本管理控制单元，一台 DNS 服务器上可以创建多个区域。如果网络规模比较大，用户数量比较多时，就可以在区域内划分多个子区域以方便管理。例如在企业中，可以为各个部分划分自己单独的子域。

(1) 在 DNS 管理器中选择要划分子域的区域，本示例中为 microsoft.com，在该区域上右击，在弹出的快捷菜单中选择“新建域”命令，打开“新建 DNS 域”对话框，输入新建子域的名称，如 news，如图 4-16 所示。



图 4-16　“新建 DNS 域”对话框

(2) 单击“确定”按钮，完成新子域的创建，此时已经可以在 DNS 管理器中看到新子域了，如图 4-17 所示。



图 4-17　“DNS 管理器”窗口

重复以上操作，可以为 microsoft.com 区域添加其他子域。但要注意，如果某个域被删除，那么它和它下属的所有子域也将同时被删除。

4.3.3　添加 DNS 记录

添加好域和子域后，DNS 服务器还不能真正的提供域名解析服务，因为此时还没有真正建立域名和 IP 地址的对应关系记录。因此还必须添加域中某服务器的名称和 IP 地址的对应关系记录，即主机记录。用户在访问网站时输入浏览器的域名，如 www.microsoft.com，就是在访问域 microsoft.com 中的名为 www 的主机。

(1) 打开 DNS 管理器，在要创建主机记录的区域名称上右击，在弹出的快捷菜单中选择“新建主机”命令，打开“新建主机”对话框，在名称文本框中输入主机名称，“完全合格的域名”文本框中将显示完整的名称，在 IP 地址文本框中输入该主机对应的 IP 地址，如图 4-18 所示。

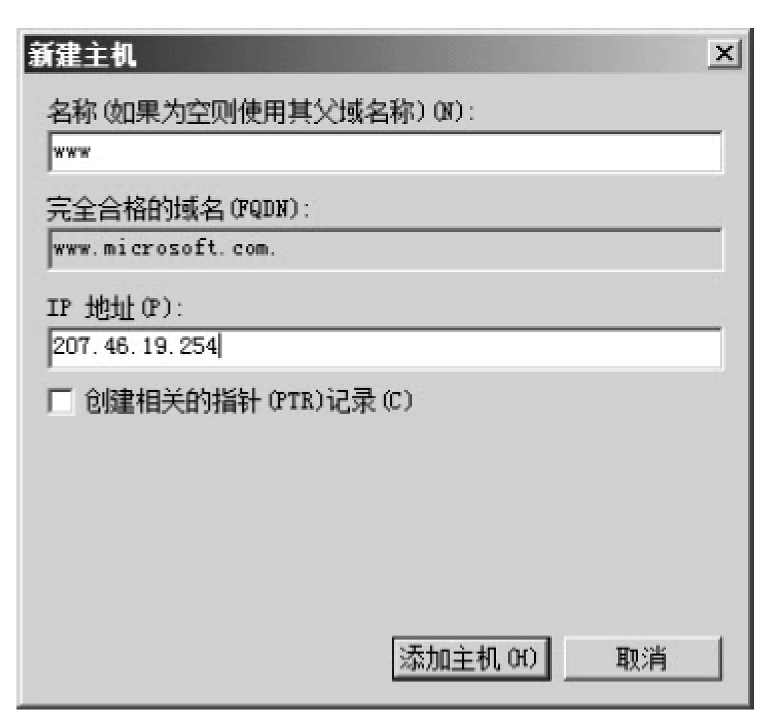


图 4-18　“新建主机”对话框

(2) 单击“添加主机”按钮，就可以完成主机 www.microsoft.com 及其 IP 地址的添加。此时用户如果访问 www.microsoft.com，当前 DNS 服务器就可以为用户提供地址解析服务了。完成添加后，系统弹出创建成功提示对话框，如图 4-19 所示。



图 4-19　创建成功提示对话框

(3) 单击“确定”按钮，弹出“新建主机”对话框，如果需要添加新的主机记录，重复上面的步骤；如果不需要添加新主机记录，单击“完成”按钮，返回 DNS 管理器，此时可以在 DNS 管理器中看到新添加的主机记录，如图 4-20 所示。

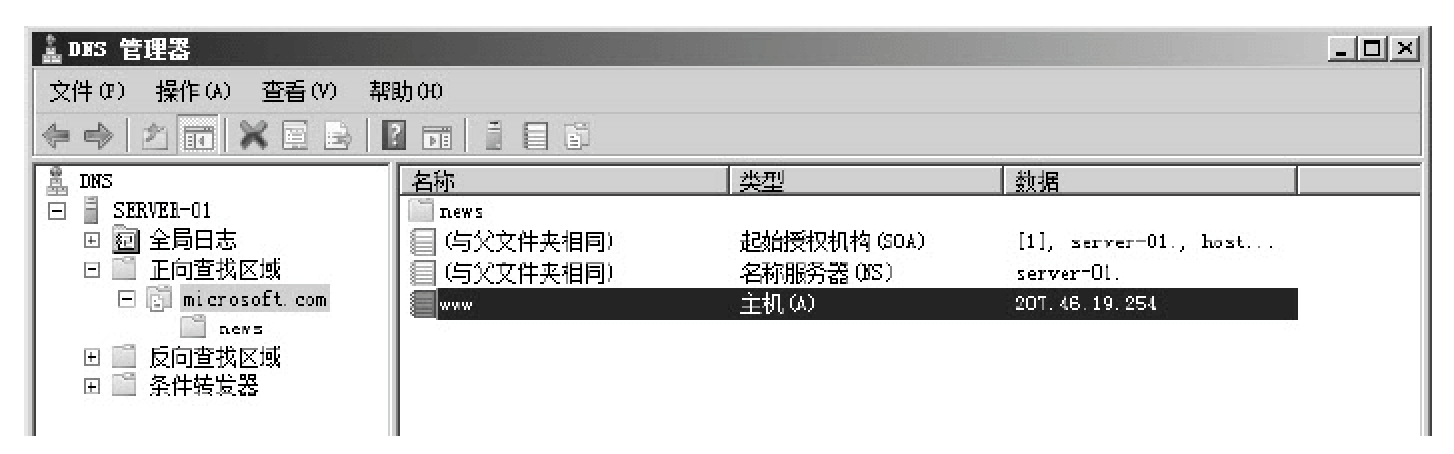


图 4-20　“DNS 管理器”窗口

4.3.4　添加反向搜索区域

反向搜索和正向搜索正好相反。正向搜索是指用户申请解析域名为 IP 地址，反向搜索则可以帮助用户将 IP 地址解析为对应的域名。网上大多数情况下进行的服务都是正向搜索，但是反向搜索也是必不可少的一项服务。

(1) 打开 DNS 管理器，右击“反向查找区域”，在弹出的快捷菜单中选择“新建区域”命令，打开“新建区域向导”对话框，如图 4-21 所示。

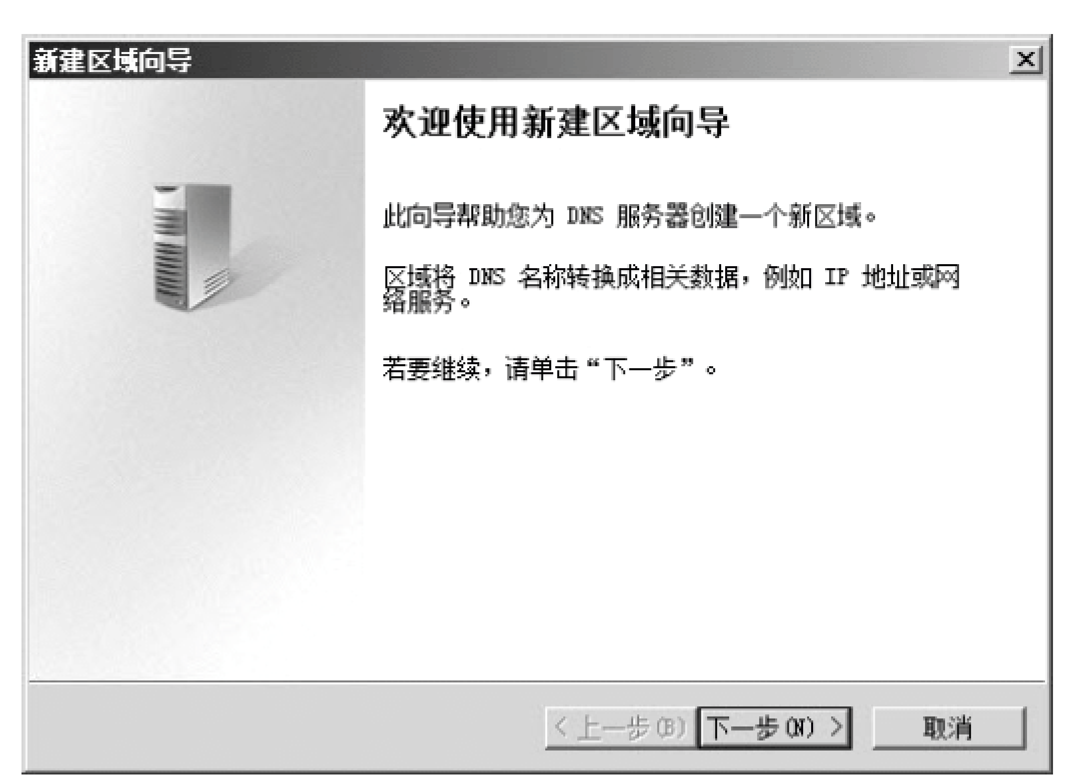


图 4-21　“新建区域向导”对话框的欢迎界面

(2) 单击“下一步”按钮，进入“区域类型”选择界面，每一项具体含义和添加正向搜索时相同。本示例选择“主要区域”，如图 4-22 所示。

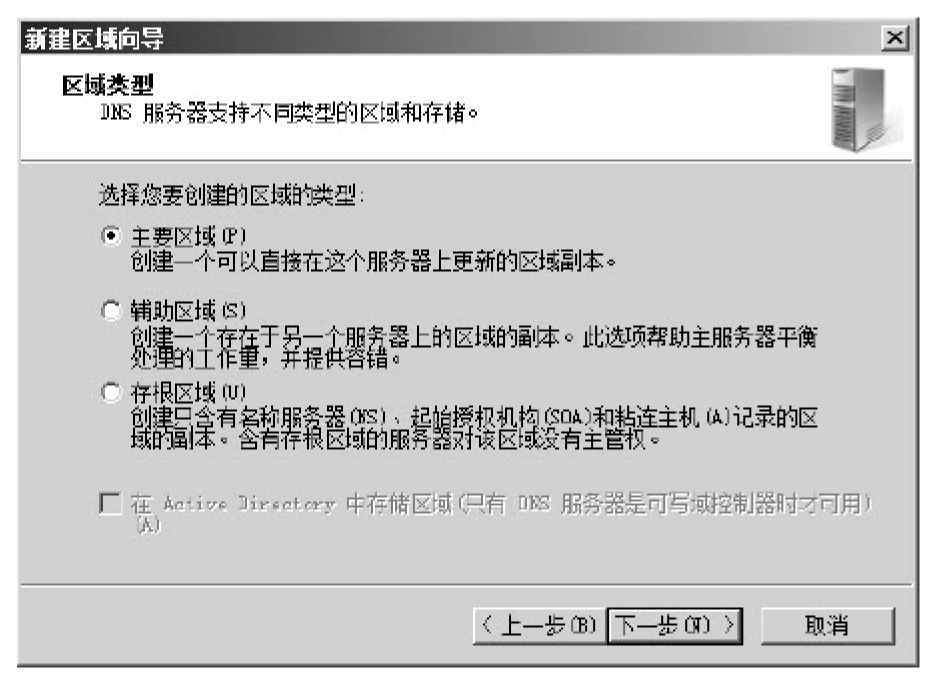


图 4-22　“区域类型”选择界面

(3) 单击“下一步”按钮，进入“反向查找区域名称”界面，选择 IP 版本，由于目前网络使用的是 IPv4，本示例选择“IPv4 反向查找区域”，如图 4-23 所示。

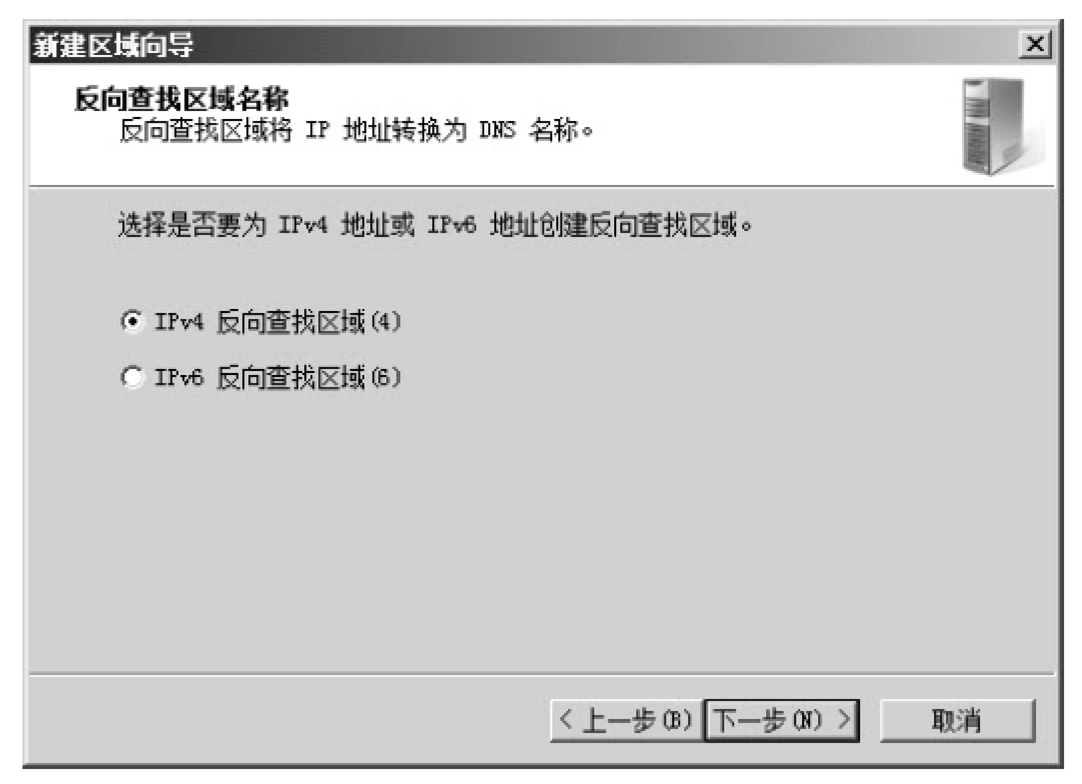


图 4-23　“地址类型”选择界面

(4) 单击“下一步”按钮，进入“反向查找区域名称”界面，标识反向查找区域，可以使用网络 ID 和方向查找区域名称两种方式。在“网络 ID”文本框中输入“207.46.19”，“反向查找区域名称”文本框会自动生成 19.46.207.in-addr.arpa 这样一个名称，如图 4-24 所示。

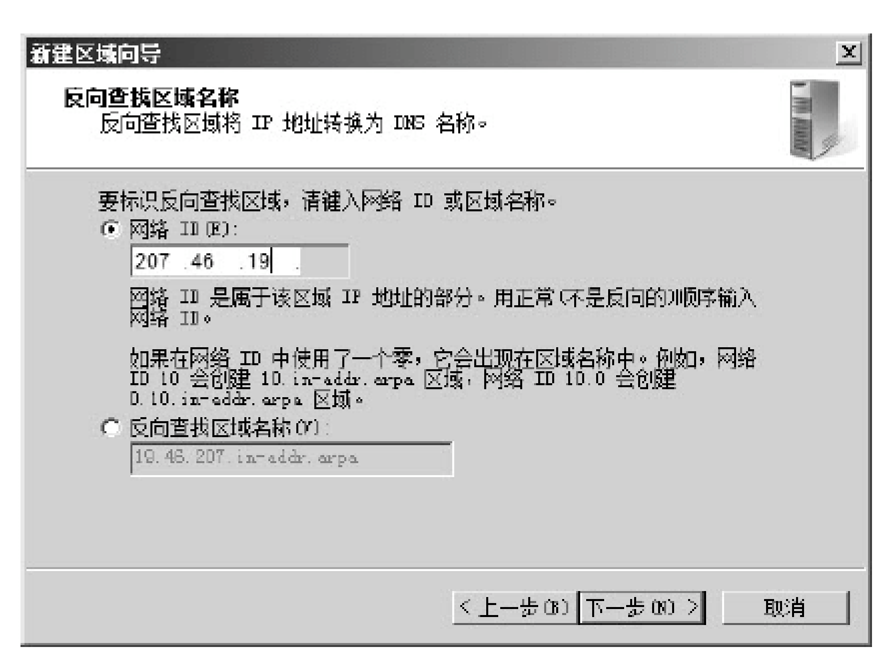


图 4-24　“网络 ID 或区域名称”界面

(5) 单击“下一步”按钮，进入“区域文件”界面，采用默认的名称命名区域文件，

如图 4-25 所示。

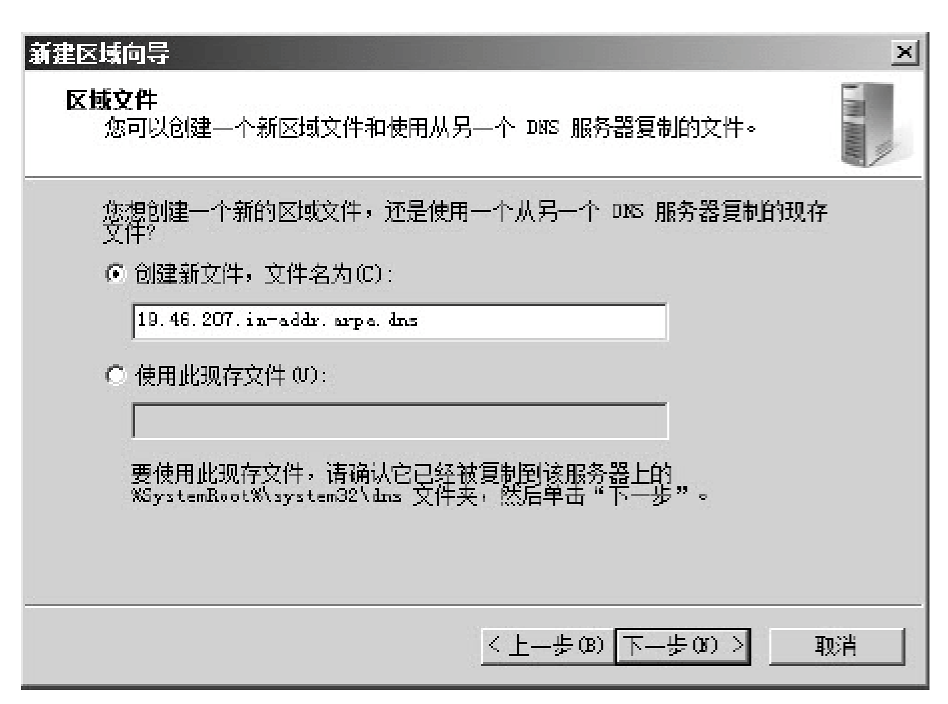


图 4-25　“区域文件”界面

(6) 单击“下一步”按钮，进入“动态更新”对话框，用来选择是否要指定这个区域接受安全、不安全或非动态的更新。为了维护 DNS 服务器的安全性，推荐选择“不允许动态更新”，如图 4-26 所示。

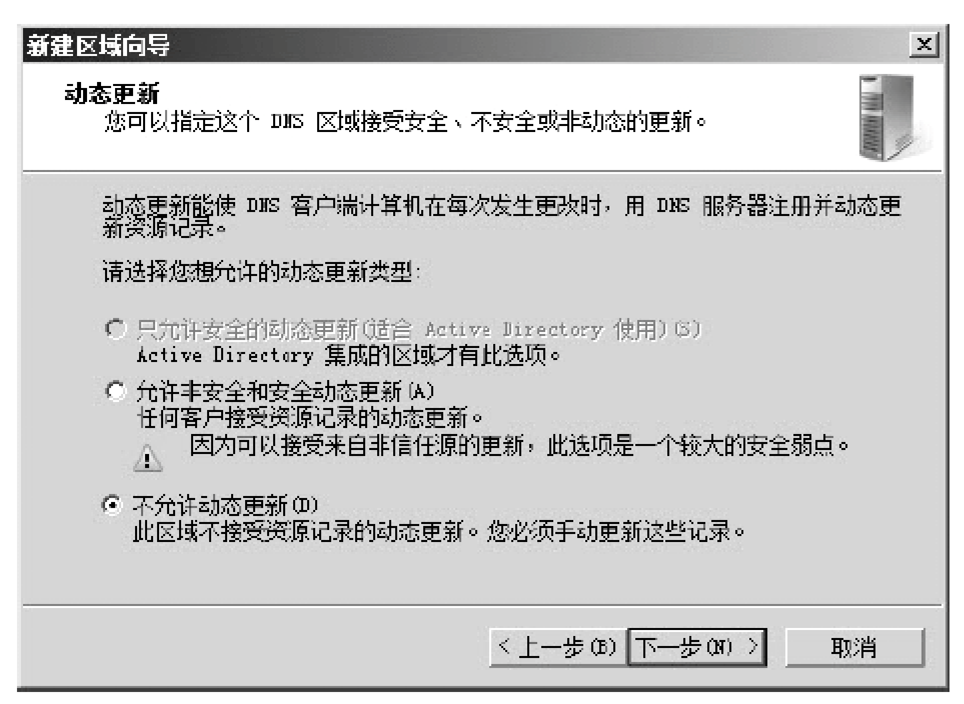


图 4-26　“动态更新”界面

(7) 单击“下一步”按钮，进入“正在完成新建区域向导”界面，如图 4-27 所示。

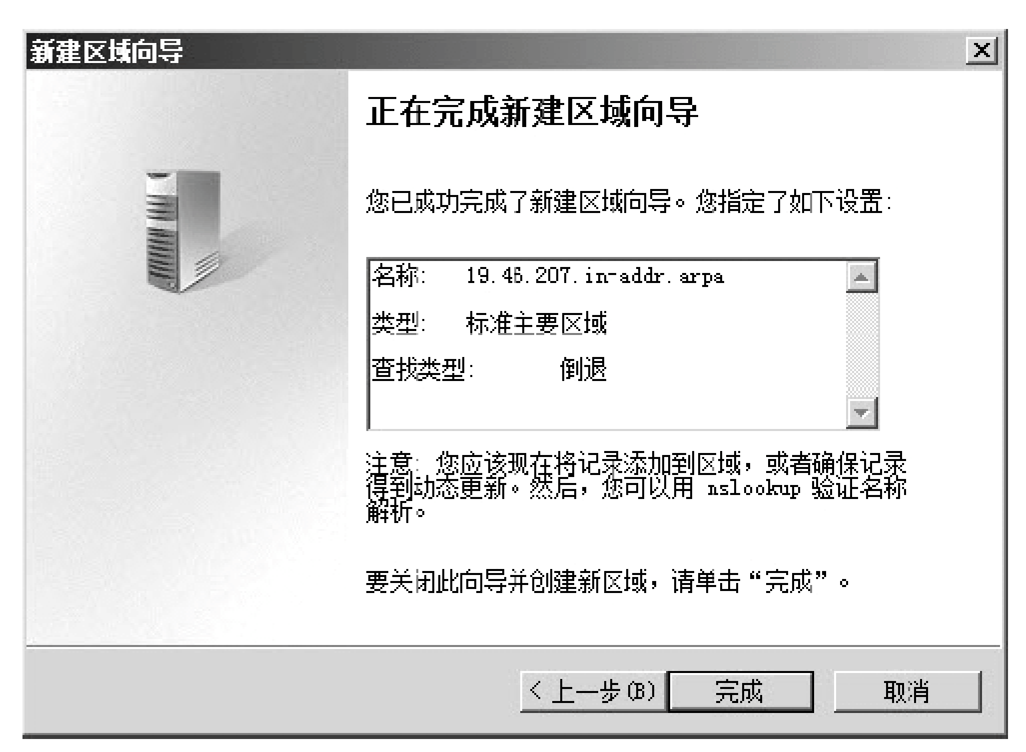


图 4-27　“正在完成新建区域向导”界面

(8) 单击“完成”按钮，关闭对话框，返回 DNS 管理器，此时 DNS 管理器中出现一

个名为“19.46.207.in-addr.arpa”反向查找区域，如图 4-28 所示。如果要添加其他反向查找区域，重复上述步骤即可。

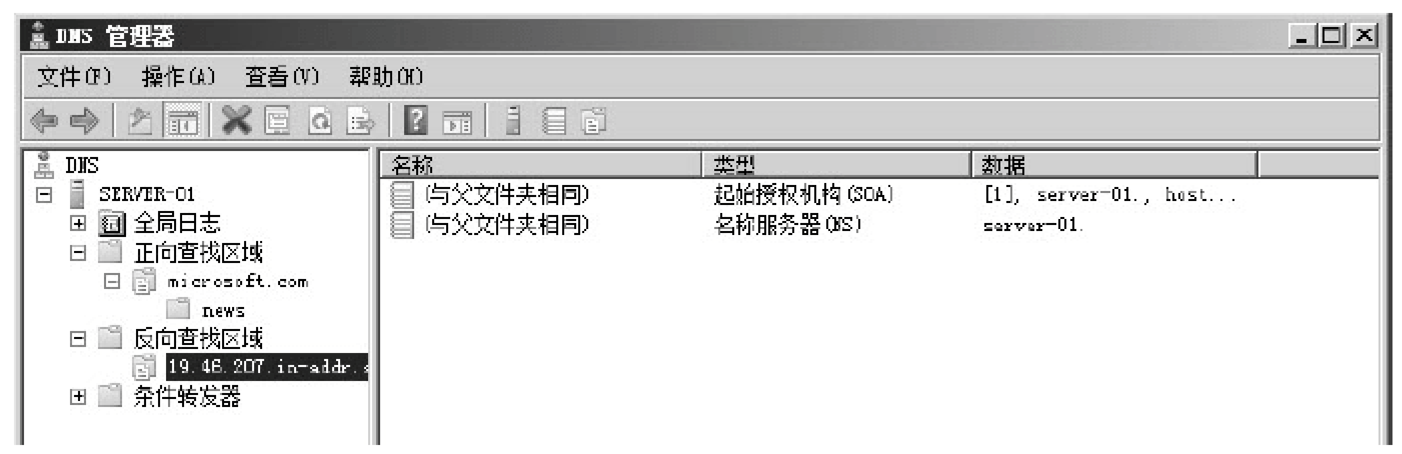


图 4-28　“DNS 管理器”窗口

(9) 创建完反向查找区域后，还需要添加反向查找记录。在 DNS 管理器中右击刚创建好的反向查找区域，从弹出的快捷菜单中选择“新建指针”命令，打开“新建资源记录”对话框，在“主机 IP 地址”文本框中输入 207.46.19.86，“主机名”文本框中输入 www.microsoft. com，或者单击“浏览”按钮选择已有的记录，如图 4-29 所示。



图 4-29　“新建资源记录”对话框

(10) 单击“确定”按钮完成添加操作，DNS 管理器中会出现刚添加好的反向查找记录，如图 4-30 所示。重复上述步骤可以添加更多的反向查找记录。

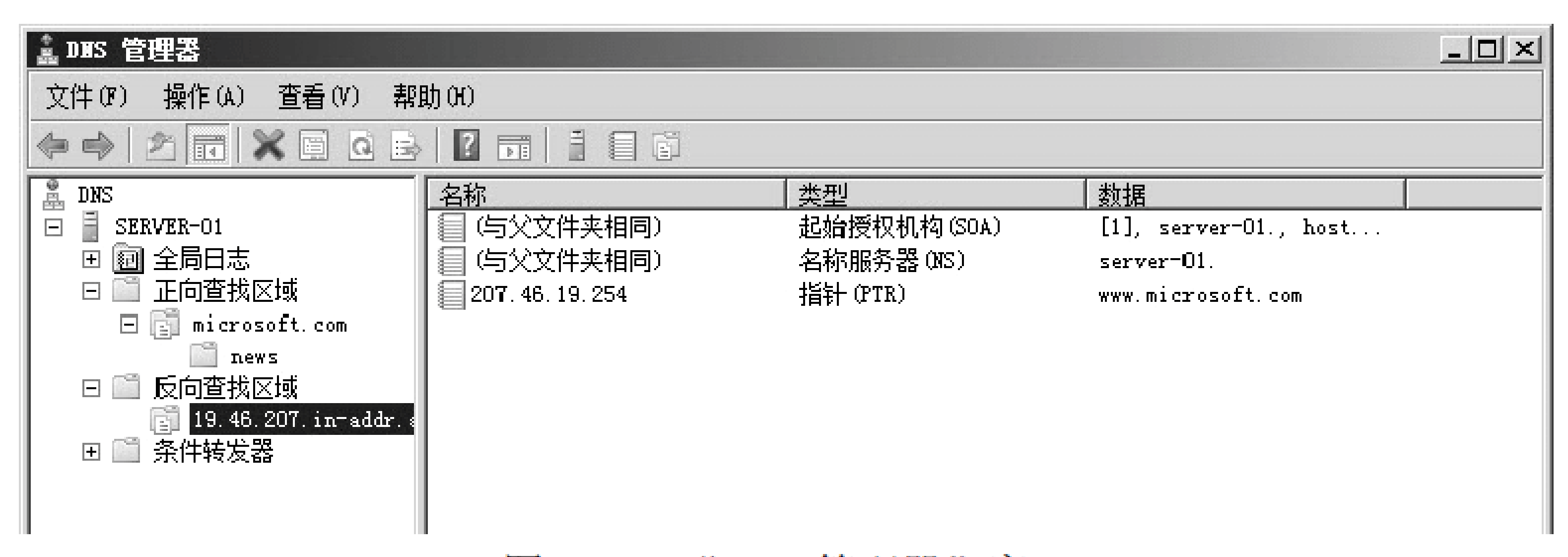


图 4-30　“DNS 管理器”窗口

4.3.5　设置转发器

任何 DNS 服务器都不可能把所有的域名都记录下来，尤其是本地网络中的 DNS 服务器，一般仅作本地服务器的地址解析或者配置活动目录使用，没有 Internet 中的网站记录。如果本地网络需要访问 Internet，比较简单的方法是在 DNS 服务器中设置一个转发器，如果 DNS 服务器遇上无法解析的域名，就将查询请求转发到其他 DNS 服务器上进行查询，从而为用户提供正确的解析服务。

(1) 打开 DNS 管理器，右击服务器名，在弹出的快捷菜单中选择“属性”命令，打开服务器属性对话框，切换到“转发器”选项卡，如图 4-31 所示。

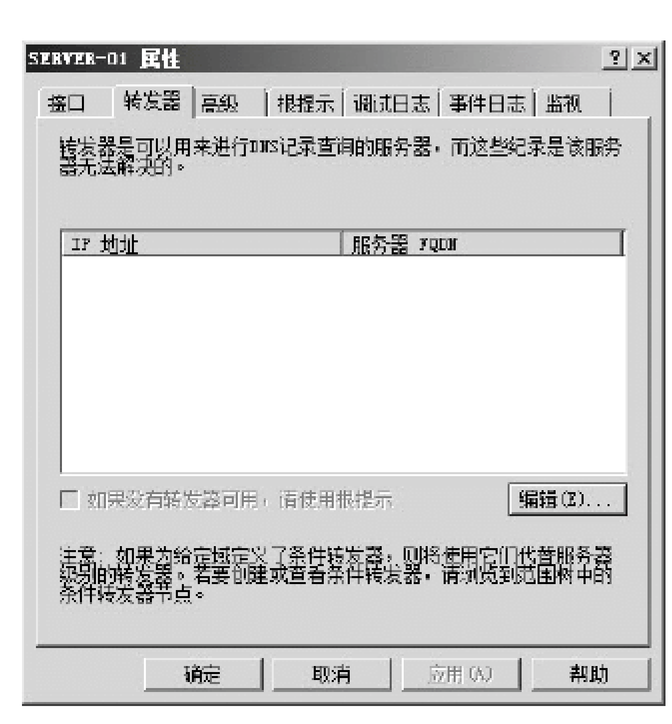


图 4-31　“转发器”选项卡

(2) 单击“编辑”按钮，打开“编辑转发器”对话框，在“<单击此处添加 IP 地址或 DNS 名称>”文本框中输入转发器的 IP 地址或 DNS 服务器的域名，按下回车键，系统会自动添加该转发器并进行验证，同时还可以输入其他转发器 IP 地址，如图 4-32 所示。

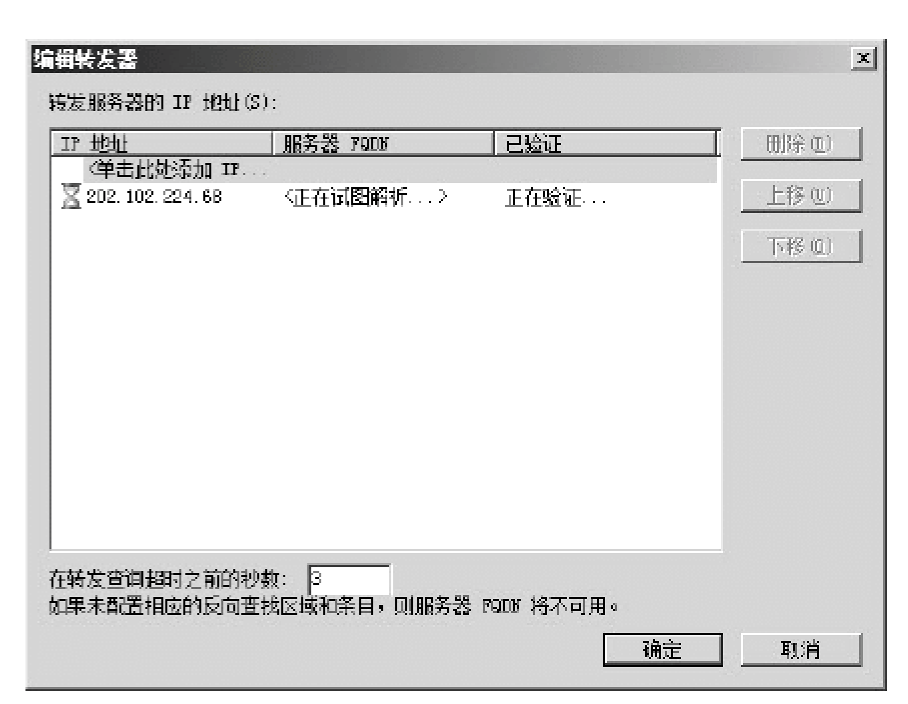


图 4-32　“编辑转发器”对话框

(3) 如果输入的转发器地址可以通过验证，单击“确定”按钮就可以将输入的转发器地址加入当前服务器的转发器列表中，如图 4-33 所示。



图 4-33　“转发器”选项卡

(4) 单击“确定”按钮，DNS 转发器设置成功，此时客户端就可以利用转发器解析当前 DNS 服务器中没有记录的域名了。

4.4　安装辅助 DNS 服务器

在一些大型网络中，为了避免由于 DNS 服务器故障导致网络不能正常使用，一般会安装两台 DNS 服务器，一台作为主 DNS 服务器，一台作为辅助 DNS 服务器。当主 DNS 服务器正常工作时，辅助 DNS 服务器只起到备份的作用，自动从主 DNS 服务器上获取 DNS 数据，如果主 DNS 服务器发生故障，辅助 DNS 服务器立即替代主 DNS 服务器承担起 DNS 解析服务。

4.4.1　配置主 DNS 服务器

在配置辅助 DNS 服务器之前，应当先在主 DNS 服务器上添加允许传送的辅助 DNS 服务器地址，并设置“通知”选项，以便主 DNS 服务器能够辅助 DNS 服务器。

(1) 以管理员帐户登录到主 DNS 服务器，打开 DNS 管理器，在要设置辅助 DNS 服务器的区域上右击，在弹出的快捷菜单中选择“属性”命令，如图 4-34 所示。



图 4-34　“DNS 管理器”窗口

(2) 打开区域属性对话框，切换到“区域传送”选项卡，选择“允许区域传送”，同时选择“只允许到下列服务器”，如图 4-35 所示。

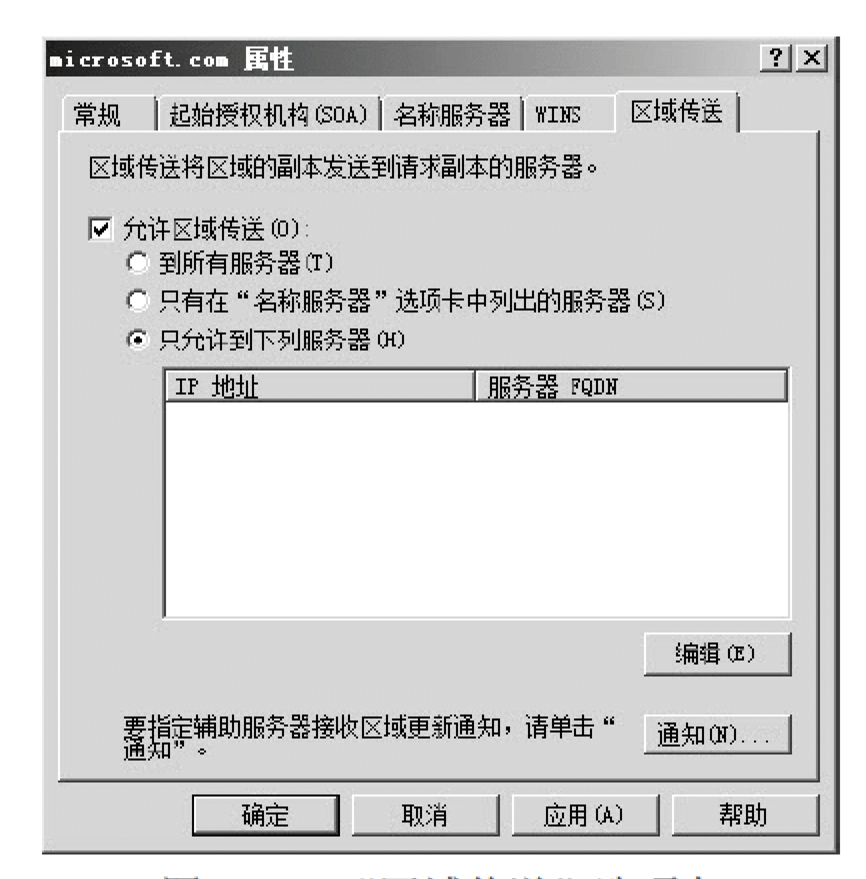


图 4-35　“区域传送”选项卡

(3) 单击“编辑”按钮，打开“允许区域传送”对话框，在“<单击此处添加 IP 地址或 DNS 名称>”文本框中输入辅助 DNS 服务器的 IP 地址或计算机名，按下回车键开始测试辅助 DNS 服务器，如图 4-36 所示。

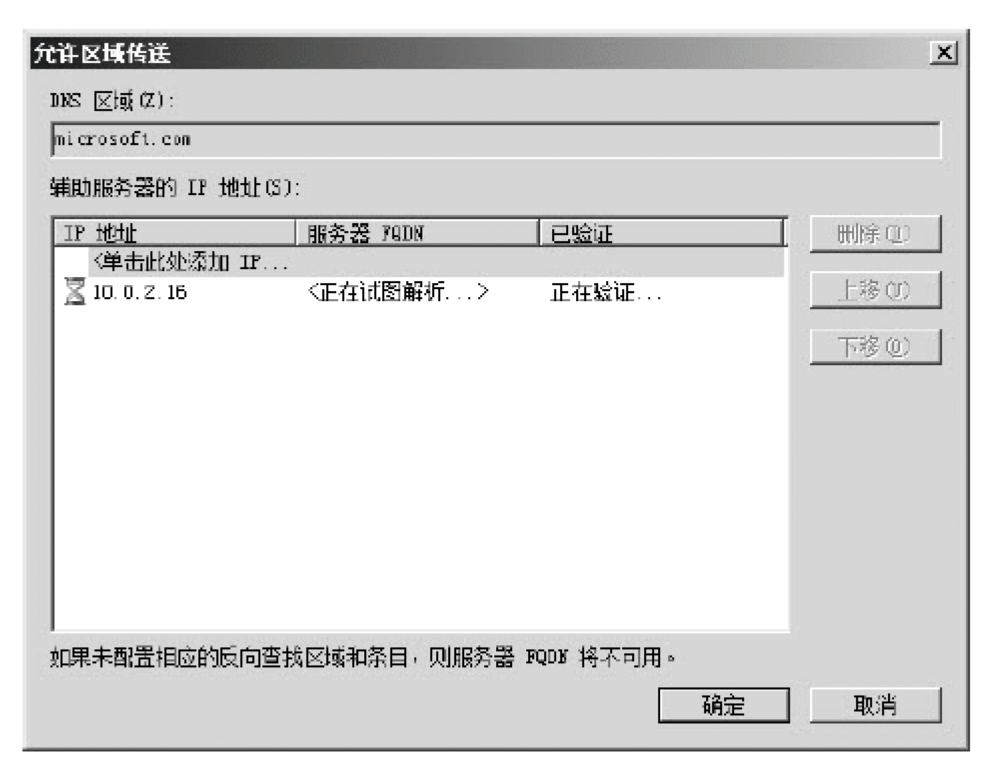


图 4-36　“允许区域传送”对话框

(4) 单击“确定”按钮，返回“区域传送”选项卡。再单击“通知”按钮，打开“通知”对话框，选择“自动通知”和“下列服务器”，在“<单击此处添加 IP 地址或 DNS 名称>”文本框中输入辅助 DNS 服务器的 IP 地址或计算机名，按下回车键开始测试辅助 DNS 服务器，如图 4-37 所示。

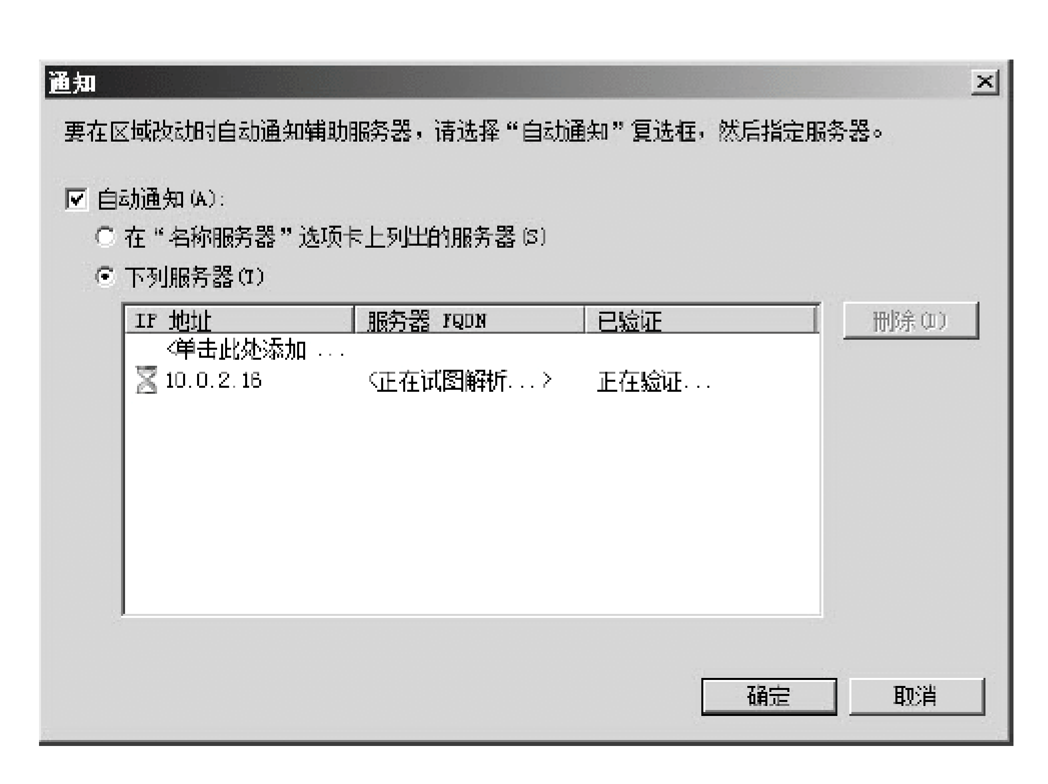


图 4-37　“通知”对话框

(5) 测试通过后，会自动返回区域属性对话框，单击“确定”按钮关闭对话框。

4.4.2　配置辅助 DNS 服务器

配置好主 DNS 服务器后，再以管理员帐户登录到辅助 DNS 服务器上进行配置。

(1) 打开 DNS 管理器，右击“正向搜索区域”，在弹出的快捷菜单中选择“新建区域”命令，打开新建区域向导；单击“下一步”按钮，在“区域类型”界面中选中“辅助区域”单选按钮，将该计算机设置为辅助 DNS 服务器，如图 4-38 所示。

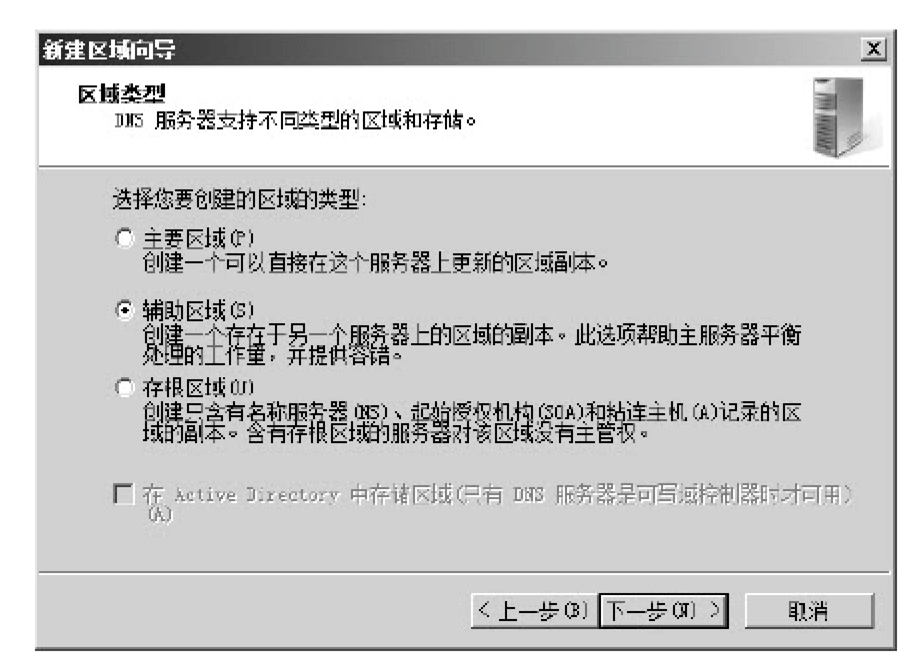


图 4-38　“区域类型”界面

(2) 单击“下一步”按钮，进入“区域名称”界面，在“区域名称”文本框中输入创建辅助区域的域名，该名称应与主 DNS 服务器上相应的名称相同，如图 4-39 所示。

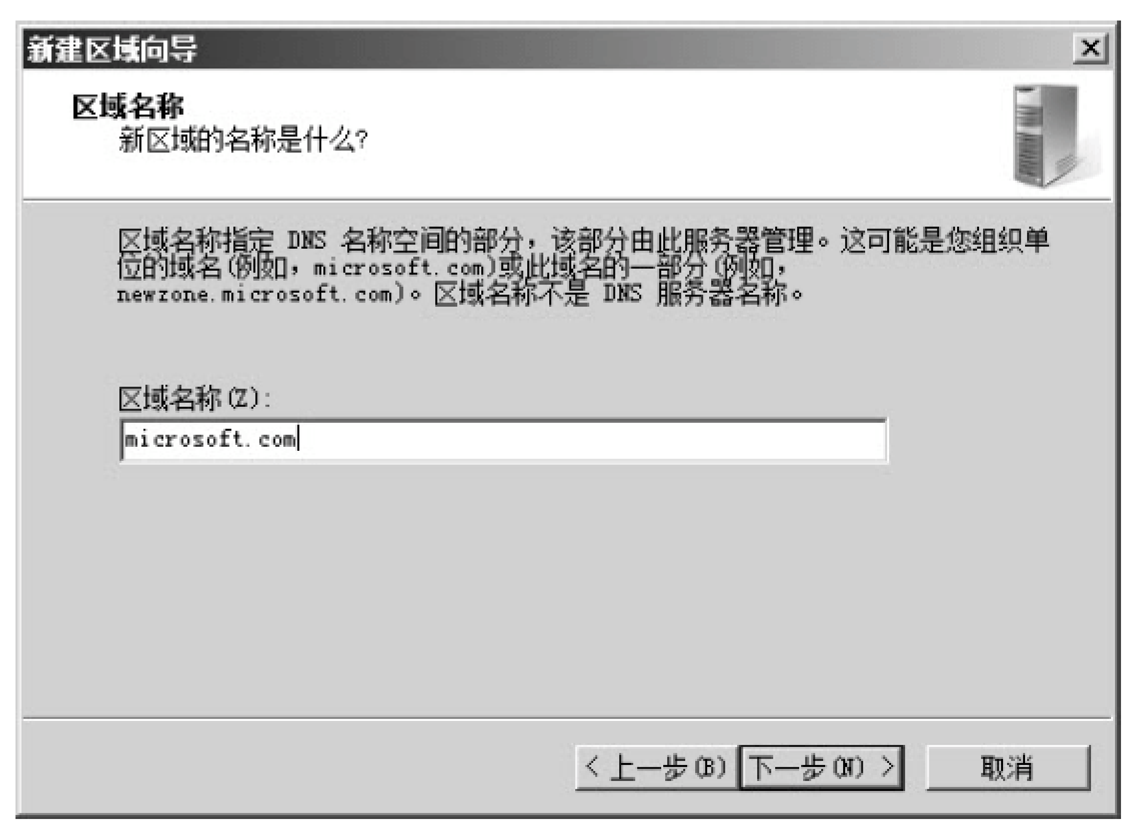


图 4-39　“区域名称”界面

(3) 单击“下一步”按钮，进入“主 DNS 服务器”界面，在“<单击此处添加 IP 地址或 DNS 名称>”文本框中输入主 DNS 服务器的 IP 地址，按下回车键开始测试，如图 4-40 所示。

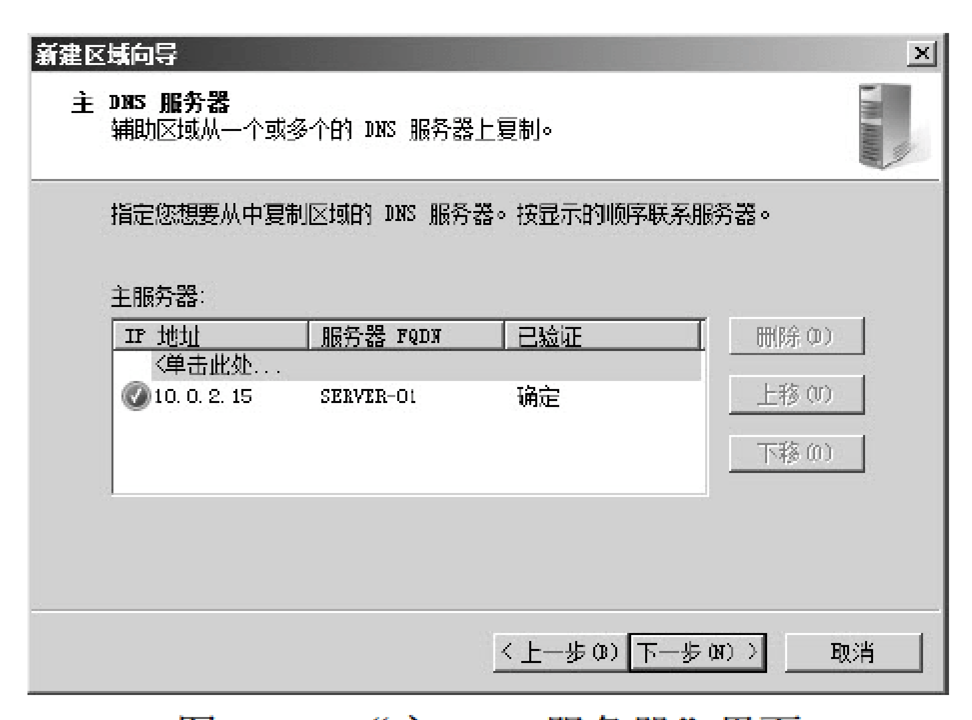


图 4-40　“主 DNS 服务器”界面

(4) 单击“下一步”按钮，显示“正在完成新建区域向导”界面，单击“确定”按钮，

辅助区域创建完毕。

辅助 DNS 服务器创建完成后，将会定时从主 DNS 服务器上同步数据，尽量和主 DNS 服务器的记录保持一致。也可以右击域名，在弹出的快捷菜单中选择“从主服务器重新加载”命令，并按 F5 键刷新记录，从而实现手动更新。

4.5　本章小结

通过本章学习，读者可以掌握 DNS 的基本工作原理和工作模式，能够配置基本的 DNS 服务器，设置客户端的 DNS 参数。

本章首先介绍了 DNS 服务的基本原理，从查询内容上看，DNS 服务的模式有正向查询和逆向查询两种，从查询方法上看，DNS 服务有递归查询和迭代查询两种。

另外，本章还介绍了安装 DNS 服务器的方法，介绍了如何在已经建好的 DNS 服务器中添加正向搜索区域和反向搜索区域，以及如何设置转发器的方法。对于客户来说，正向 DNS 查询是主要的，使用频繁，反向查询则要少很多。DNS 服务器也不可能记录网络上所有的域名记录，因此还需要利用转发器使 DNS 服务器之间也可以进行记录查询。

最后介绍了辅助 DNS 服务器的安装方法。在大型网络或业务较繁忙的网络中，必须保证用户随时可以使用 DNS 服务，此时可以在网络中再布置一台或更多的辅助 DNS 服务器，作为主要 DNS 服务器的候补，在主 DNS 服务器出现问题时依然可以提供正常服务。

4.6　思考与练习

【思考题】

1. 在企业网络中 DNS 服务器能起到什么作用？
2. 在内网连接外网这一环节上，如何快速设置 DNS 服务器？

【练习题】

1. 简述 DNS 服务的基本流程。
2. DNS 服务的工作模式有哪些？
3. 简述辅助 DNS 服务器的作用是什么？
4. 辅助 DNS 服务器如何同步主 DNS 服务器上的数据？

第5章　活动目录服务

【本章导读】

Active Directory(R)域服务(AD DS)是 Windows Server 2008 操作系统的一个服务器角色。AD DS 提供分布式目录服务，用于存储网络上各种对象的相关信息，如计算机、用户、打印机、服务器等，并使用一种易于用户查找及使用的结构化的层次结构数据存储方法来组织和保存数据，以便于管理员查找和使用；在整个目录中，通过登录验证以及目录中对象的访问控制，将安全性集成到 Active Directory 中，可以使用该服务对网络进行集中安全管理。

5.1　活动目录概述

Windows Server 2008 活动目录域服务(AD DS)有了很大的改进。主要表现在新增了只读域控制器(RODC)的域控制器类型、更新的活动目录域服务安装向导、可重启的活动目录域服务、快照查看以及增强的 Ntdsutil 命令等。由于这些改进，现在可以通过新的安装向导简化部署过程并节省部署时间；可以在物理安全无法得到保证的分支机构部署 RODC；还可以使用 AD DS 的可重启功能来停止 AD DS，因此可以执行诸如脱机的活动目录对象整理之类的脱机操作，减少了在 Windows Server 2008 下需要重启至活动目录还原模式的次数。通过快照查看还可以在线查看存储在快照中的活动目录数据，虽然不能使用此特性来还原已删除的对象和容器，但是可以在不重启域控制器的情况下，使用它来比较不同时间点的快照以确定用哪份数据进行恢复。

5.1.1　活动目录服务的功能

目录服务可以实现如下功能：

(1) 提高管理者定义的安全性来保证信息不受入侵者的破坏；

(2) 将目录分布在一个网络中的多台计算机上，提高了整个网络系统的可靠性；

(3) 复制目录可以使得更多用户获得它并且减少使用和管理开销，提高效率；

(4) 分配一个目录于多个存储介质中，使其可以存储规模非常大的对象。

Active Directory 服务包括证书服务(AD CS)、域服务(AD DS)、联合身份验证服务(AD FS)、轻型目录服务(AD LDS)和权限管理服务(AD RMS)。功能如下：

(1) Active Directory Certificate Services(证书服务)：允许创建、分发和管理自定义公钥证书。通过将个人、设备或服务的标识与相应的私钥进行绑定，组织可使用 AD CS 来增

强安全性。AD CS 为组织提供了一种对证书的分发和使用进行管理的经济、高效和安全的方法。AD CS 所支持的应用领域包括安全/多用途 Internet 邮件扩展(S/MIME)、安全的无线网络、虚拟专用网络(VPN)、Internet 协议安全(IPsec)、加密文件系统(EFS)、智能卡登录、安全套接字层/传输层安全性(SSL/TLS)以及数字签名。

(2) Active Directory Domain Services(AD DS 域服务)：存储目录数据以及管理用户与域之间的通信，包括用户登录过程、身份验证和目录搜索。通过应用 Windows Server 2008 的域服务器角色，可以为用户和资源管理创建一个大规模的、安全的、可管理的架构，并且可以支持目录驱动的应用程序，比如 Microsoft Exchange Server。

(3) Active Directory Federation Services(AD FS 联合身份验证服务)：可用来创建可高度扩展、可伸缩和安全的身份访问解决方案，此解决方案可在多个平台上工作，包括 Windows 和非 Windows 环境，提供 Web 单一登录(SSO)技术以在单个联机会话期间为多个 Web 应用程序对用户进行身份验证。

(4) Active Directory Lightweight Directory Services(AD LDS 轻型目录服务)：是一种轻型目录访问协议(LDAP)，可以灵活地支持启用目录的应用程序，并且不受 Active Directory 域服务(AD DS)的限制。AD FS 是一个身份访问解决方案，即使用户帐户和应用程序分别处于完全不同的网络或组织中，它也使基于浏览器的客户端(网络内部或外部)能够对一个或多个面向 Internet 的受保护应用程序进行无缝的“一次提示”访问。

当应用程序处于一个网络中而用户帐户处于另一个网络中时，用户在尝试访问该应用程序时通常会遇到要求输入辅助凭据的提示。这些辅助凭据代表应用程序所驻留的领域中的用户身份。承载该应用程序的 Web 服务器通常需要这些凭据，以便能够作出最适当的身份认证决策。

AD FS 通过提供信任关系来避免使用辅助帐户及其凭据，可以使用此信任关系将用户的数字身份和访问权限投影到受信任的伙伴。在联合的环境中，每个组织除了能继续管理自己的身份外，还能安全地投影和接受来自其他组织的身份。

此外，可以将联合身份验证服务器部署在多个组织中，以便简化受信任伙伴组织之间的企业对企业(B2B)事务。联合的 B2B 合作关系将商业伙伴识别为下列组织类型之一。

- 资源组织。如果组织拥有并管理可从 Internet 访问的资源，则可以部署 AD FS 联合服务器和启用 AD FS 的 Web 服务器，这些服务器管理受信任伙伴对受保护资源的访问。这些受信任的伙伴可以包括外部的第三方或同一组织中的其他部门或分支机构。
- 帐户组织。如果组织拥有并管理用户帐户，则可以部署对本地用户进行身份验证的 AD FS 联合服务器，并创建资源组织中的联合服务器，之后可以做出授权决策的安全令牌。

在访问其他网络中的资源时，对一个网络进行身份验证的过程称为单一登录(SSO)，它消除了重复登录操作的负担。AD FS 提供基于 Web 的 SSO 解决方案，该解决方案在一个浏览器会话的整个期间针对多个 Web 应用程序对用户进行身份验证。

(5) Active Directory Rights Management Services(AD RMS 权限管理服务)：决定了如何保护信息，以及如何与启用 AD RMS 的应用程序协同工作，帮助防止在未经授权的情况下使用数字信息。

5.1.2　活动目录结构

活动目录包括两方面：目录和目录相关的服务。目录是一个物理上的存储各种对象的容器，目录管理的基本对象是用户、计算机、文件以及打印机等资源对象。而目录服务是使目录中所有信息和资源发挥作用的服务，如用户和资源管理、基于目录的网络服务、基于网络的应用管理。活动目录是一个分布式的目录服务，信息可以分散在多台不同的计算机上，保证快速访问和容错；同时，不管用户从何处访问或信息处在何处，对用户都提供统一的视图。

AD DS 的逻辑结构是由域、组织单元、树和树林、全局编录等多个组件组合而成的。

1. 域

域又称域目录，是将网络中多台计算机在逻辑上组织到一起，进行集中管理，是共享同一活动目录的一组计算机的集合。这种区别于工作组的逻辑环境称为“域”。域是 Windows 的逻辑管理单元，是一系列的用户帐户、访问权限和其他各种资源的集合。域是安全的边界，在默认情况下，域管理员只能对本域范围内的对象进行管理，不能管理其他域，除非被明确分配了对其他域拥有的管理权利。

可从以下应用实例中体会域的作用：在基于 Windows 工作组功能而构建的对等网络(通常为小型网络)中，资源分布在多台服务器上，要在每台服务器分别为每一员工建立一个帐户(共 m×n)，用户则需要在每台服务器上(共 m 台)登录，如图 5-1 所示，因此，基于工作组的对等网络通常为小型网络。

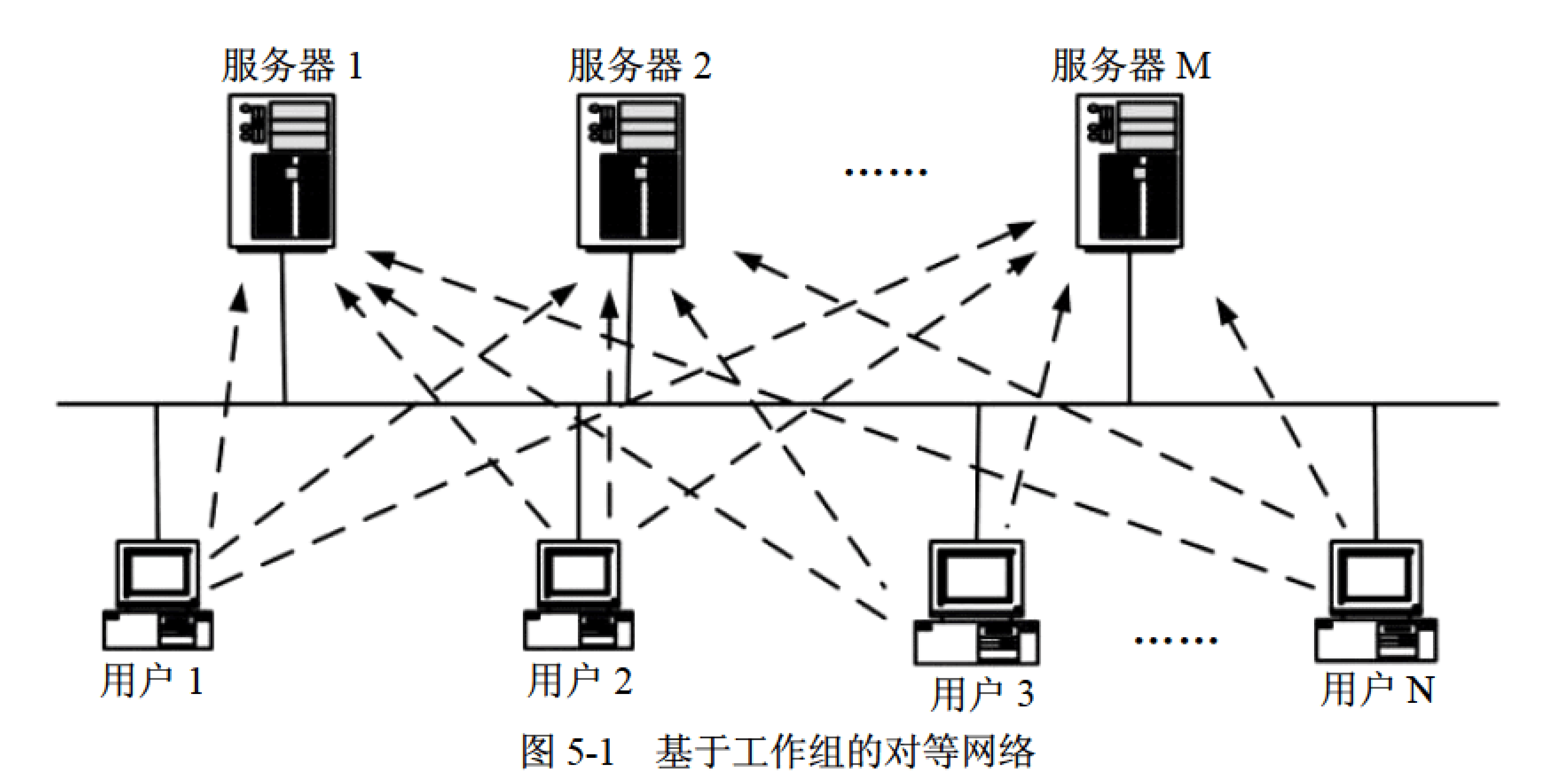


图 5-1　基于工作组的对等网络

如图 5-2 所示，在基于 Windows 域服务的功能而构建的网络中，服务器和用户的计算机都在同一个域中，用户只需要在域中拥有一个域帐户，只需要在域中登录一次就可以访问域中的资源了；可见，域可以组建大型的网络，而且简化了网络管理，方便了网络用户。

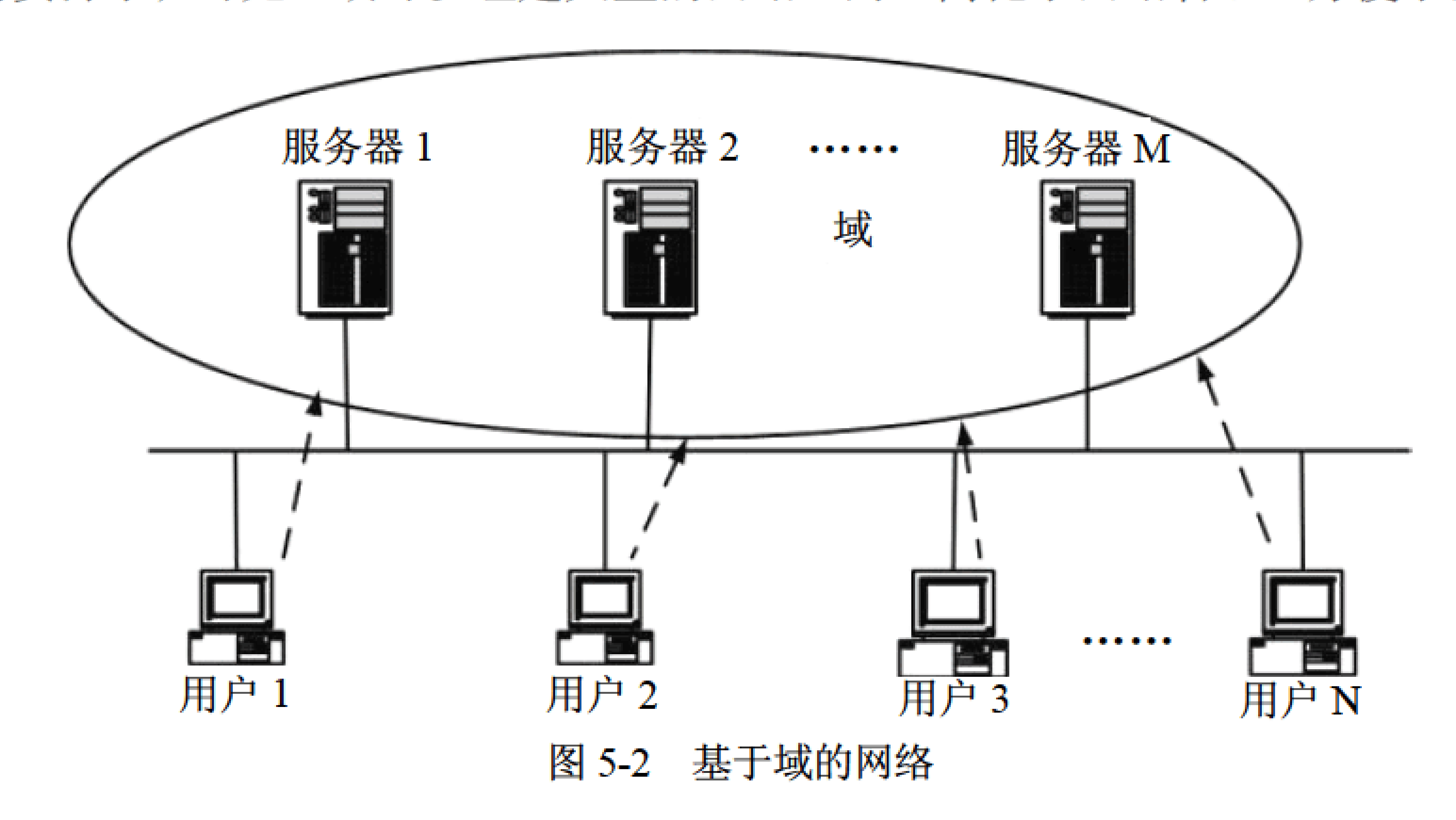


图 5-2　基于域的网络

用点分字符串结构表示域的名称，如某公司的域名为 ms.com。

在一个域中，通过运行 Active Directory 来发挥对域的管理、控制作用的服务器称为域控制器，活动目录的所有信息(包括用户帐号和安全数据库)存储在域控制器内。域控制器一般是一台服务器级别的计算机，在 Windows Server 2008 家族中，除 Windows Web Server 2008 外，其他都可以扮演域控制器的角色。

由于在域控制器上，Active Directory 存储了所有的域范围内的帐户和策略信息，如系统的安全策略、用户身份验证数据和目录搜索。帐户信息可以属于 3 种对象之一：用户、服务和计算机。

注意：

由于有 Active Directory 的存在，域控制器不需要本地安全帐户管理器(SAM)，即域控制器上的登录不仅仅是登录本机，全是登录到整个域中。

一个域可包含多个域控制器，每一台域控制器的地位(几乎)是平等的，各自存储着一份几乎完全相同的活动目录数据库。当某个域控制器的活动目录数据库修改以后，会将此修改复制到其他所有域控制器，以便让所有域控制器内的 AD DS 数据都能够同步。比如，当在任何一台域控制器内添加一个用户帐户后，这个帐户默认是被创建在此域控制器的活动目录数据库内，之后这份帐户数据会自动被复制到其他域控制器的活动目录数据库内，实现了域控制器之间信息的同步更新。

多台域控制器可以提高系统的可靠性，提供容错功能，同时可以改善登录效率。

域控制器之间在复制活动目录数据库时，其复制方式可以分为以下两种模式。

(1) 多主机复制模式(Multi-master Replication Model)

活动目录数据库内的大部分的数据(如上述帐户数据的复制)都是利用这种模式在复制。

(2) 单主机复制模式(Single-master Replication Model)

当提出更改对象数据的请求的时候，会由其中一台域控制器(操作主机)负责接收与处

理此请求，也就是说该对象是先被更新在操作主机，再由这台操作主机将它复制到其他域控制器。

域中除域控制器外，通常还有其他成员计算机，要充分管理计算机，需要将这些计算机加入到域内。比如，用户要使用活动目录数据库内的域用户帐户来登录，这些计算机也必须加入域。没有加入域的计算机只能够使用本地用户帐户登录。

域中其他成员计算机包括成员服务器、独立服务器和客户端计算机。

- 成员服务器

服务器级别的计算机加入域后被称为成员服务器，成员服务器的区别不是硬件，而是操作系统。成员服务器可以是：

Windows Server 2008

Windows Server 2003

Windows Server 2000

- 独立服务器

若上述服务器没有加入到域，则被称为独立服务器或工作组服务器。独立服务器或工作组服务器都有本地的 SAM(Security Accounts Manager)，系统可以用 SAM 来审核本地的用户身份。

- 客户端计算机

包括：

Windows Vista Ultimate

Windows Vista Enterprise

Windows Vista Bussiness

Windows XP Professional

注意：

Vista home premium、Vista home basic、Vista starter、XP home edition 等计算机在登录窗口中无法选择域用户来登录，只能利用本地用户帐户来登录。

在 Windows 网络环境下，可以将独立服务器或成员服务器升级成为域控制器，也可以将域控制器降级为独立服务器或成员服务器。

2. 组织单元(Organizational Unit，OU)

组织单元是一个比较特殊的容器。一个组织单元可以包括用户、计算机、文件以及打印机等资源对象与其他组织单元，还有组策略功能，即通过作用于本单元内的策略来管理资源对象与其他组织单元。通过为用户或组分配特定的权限，从而给其委派对某个 OU 中的对象进行管理控制的能力。

3. 域树

一个组织单元，如公司，通常有包含若干个二级部门，如财务部、销售部等，有的二

级部门下还包括若干个三级部门，如销售部包括河南销售科和河北销售管科等。大型单元的各个部门为了提高自身信息的管理效率，通常都有自己的域，与上级部门的域形成层次关系，下级部门的域名以上级部门的域名为后缀，如上述公司销售部的域名为 sales.ms.com，河南销售科的域名为 henan.sales.ms.com，河北销售科的域名为 hebei.sales.ms.com。如图 5-3 所示，最上层的域为根域，根域的下级域称为它的子域，根域和它的各层次子域组成了一个树状结构，该结构称为“域树”。一个域树只有一个名字，取名为根域的名字。

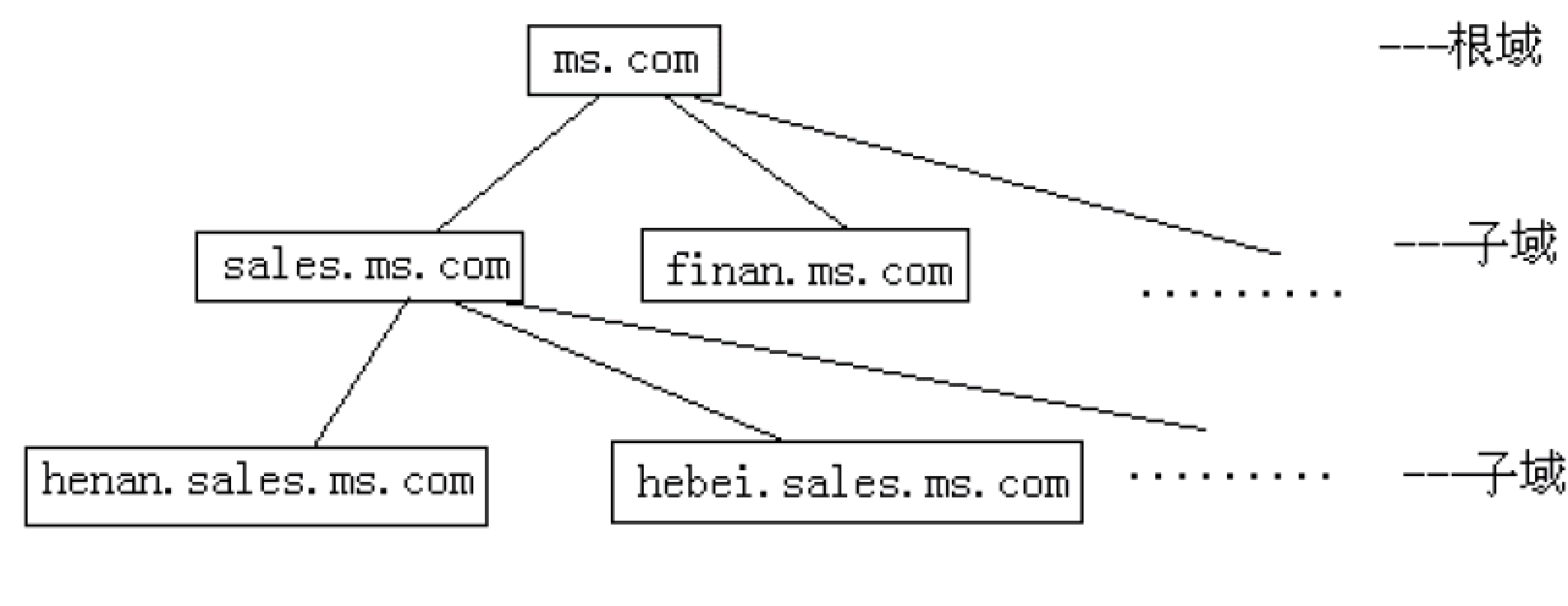


图 5-3　域树

域树内的根域和它的所有子域共享一个活动目录数据库，不过这个活动目录数据库内的数据分散地分布在各个域内，每个域只存储属于该域的数据。

域树内的一个域与子域之间用信任关系建立联系。两个域建立信任关系后一个域中的主机才可以访问对方域内的资源。当一个域的域服务器被加入到域树的活动目录数据库后，这个域会自动信任父域，同时父域也自动信任这个新加入的子域，而且这种信任关系具有双向传递性(Two-way Transitive)。因为传递性得到的信任关系，称为隐性的信任关系。所以，当任何一个子域加入到域树后，它会自动双向信任这个域树内的所有域，因此只要拥有适当权限，这个新域内的用户便可以访问其他域的资源，同理，其他域内的用户也可以访问这个新域内的资源。

另一方面，按照功能的不同，可以将目前的域划分为三个级别：Windows 2000 域、Windows Server 2003 域和 Windows Server 2008 域。一个域的功能级别的设置只影响到该域，不会影响到其他域。

Windows 2000 域内的域控制器上使用的操作系统版本可以是：Windows 2000 Server、Windows Server 2003 或 Windows Server 2008。

Windows Server 2003 域内的控制器可以是：Windows Server 2003 或 Windows Server 2008。

Windows Server 2008 域内的域控制器只能是：Windows Server 2008。

注意：

可见，域内的域控制器上操作系统的版本不能比域级别低，但可以比域级别高。可以提升域的功能级别。比如将 Windows 2000 域的功能级别提升到 Windows Server 2008。一

旦提升后，不能再被降级。

4. 域树林

域树林由一个或多个域树组成，如图 5-4 所示，域树林中创建的第一个域树，其根域就是整个域树林的根域，同时该根域的名称就是域树林的名称。各域树之间地位相当，由双向传递的信任关系相关联；当创建域树林时，一个域树内的根域与其他域树内的根域之间双向的、传递性的信任关系都会被自动创建。因此，每个域树中的每个域内的用户，只要拥有权限，都可以登录到其他任何一个域树内各个域的计算机，访问计算机的资源。

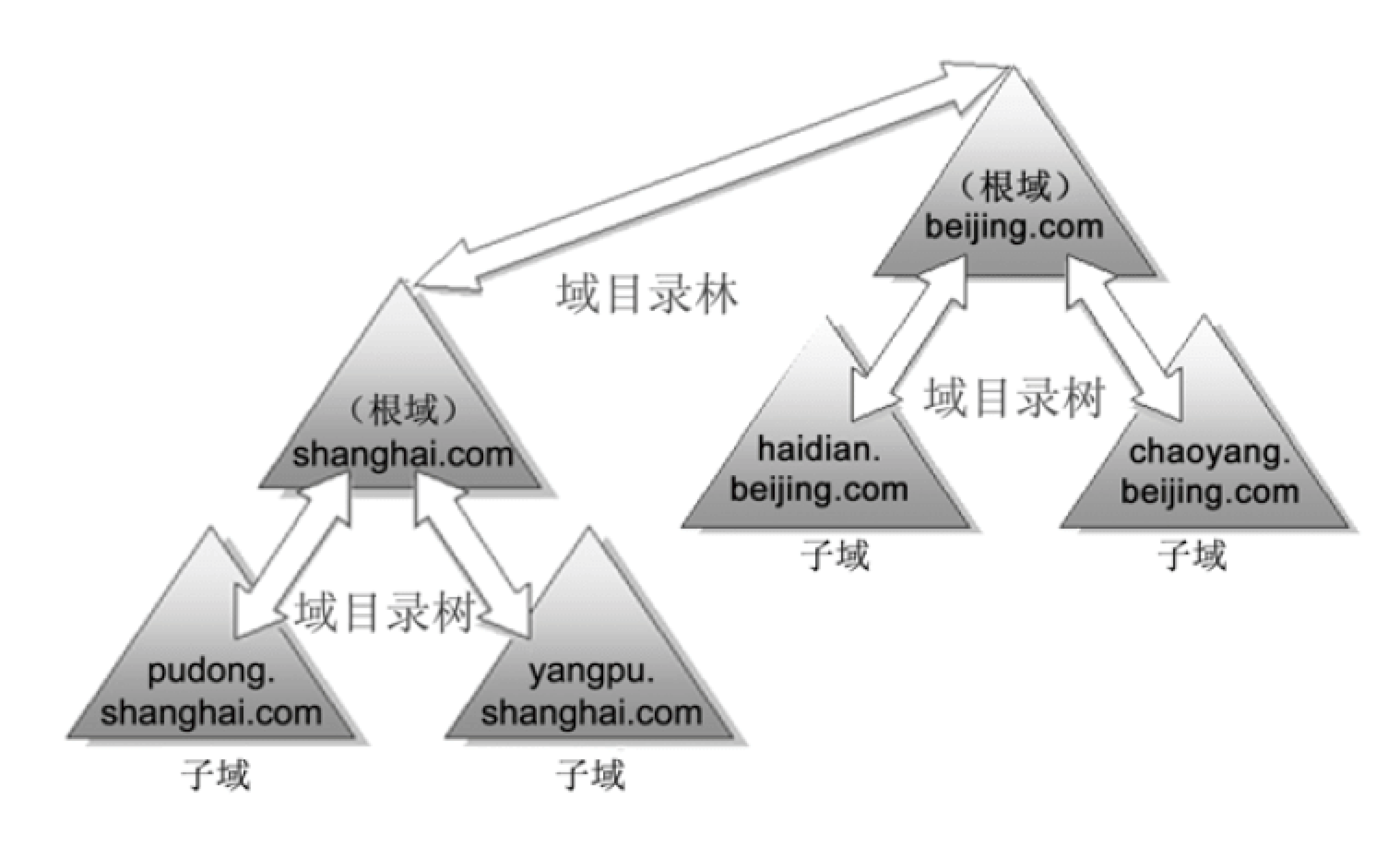


图 5-4　树林

单独的一个域组成仅包含一个域的域树，单独的一个域树组成仅包含一个域树的域树林。

另一方面，与功能级别类似，一个域树林的功能级别的设置只影响到该域树林，不会影响到其他域树林。但在 Windows Server 2008 域树林的功能级别之内所添加的域，其域功能级别会被设置为 Windows Server 2008。

5. 全局编录

虽然在域树内的所有域共享一个活动目录数据库，但是活动目录数据库内的数据确实分散在各个域内，而且每个域只存储域本身的数据。为了让用户、应用程序能够迅速地找到位于其他域的资源，设计了全局编录。

全局编录的数据是存储在域控制器内的，这台域控制器被称为全局编录服务器，其存储着林内所有域的活动目录数据库内的每一个对象，不过只存储每一个对象的部分属性，这些属性都是常被搜索的属性。

用户登录的时候，全局编录服务器负责提供该用户所隶属的全局组数据。当用户用 username@ms.com 登录时，它负责提供该用户是属于哪一个域的信息。

一个林内的所有域树目录共享相同的全局编录，而林内的第一台域控制器默认为全局编录服务器。也可以指派其他域控制器为全局编录服务器。

6. 轻型目录访问协议(LDAP)

轻型目录访问协议是用来访问活动目录数据库的目录服务协议。活动目录是利用 LDAP 名称路径(LDAP Naming Path)来表示对象在活动目录数据库中的位置，以便用它来访问活动目录数据库内的对象。

注意：

站点与域不同。域代表组织的逻辑结构，而站点代表网络的物理结构，因为一个站点可以跨越多个域，而一个域也可以跨越多个站点。站点并不属于域名称空间的一部分，站点控制域信息的复制，并可以帮助确定资源位置的远近。

站点是由一个或多个 IP 子网所组成的，这些子网之间通过高速且可靠的链路串接起来，如果链路不满足要求，应该将其划为不同的站点。例如，一个 LAN 内的各个子网之间的链路都是高速且可靠的链路，而通过 WAN 互联的站点速度一般不快，所以应该划分为多个站点。

域是逻辑的分组，而站点是物理的分组，在活动目录内，一个站点可能会含有多个域；而一个域内的计算机也可能分别属于不同的站点。

如果一个域的域控制器分布在不同的站点内，且这些站点是低速连接，由于两个域控制器之间因为需要同步数据而需要复制数据，所以需要谨慎规划数据复制的时间段，尽量设置在非高峰时期来执行复制工作，同时复制频率也不要太高，以避免复制时占用两个站点之间的链接带宽，影响两个站点之间的数据传输。隶属于同一个站点之间的域控制器会自动执行复制功能，默认的复制频率也比较高。

不同站点之间的数据进行复制的时候，所传送的数据会被压缩，同一个站点之间的数据不会被压缩。

5.2　活动目录的配置与删除

5.2.1　安装前的准备

首先，在安装活动目录之前，必须保证已经有两台计算机(假设分别名为 W2K8S1 和 W2K8S2)安装了 Windows Server 2008，且至少有一个 NTFS 分区，已配置适当的 IP 地址和 DNS 服务器，并且 DNS 服务支持服务器记录和动态更新协议。

其次，要规划好整个系统的域结构，活动目录可包含一个或多个域，如果整个系统的目录结构规划得不好、层次不清，就不能很好地发挥活动目录的优越性。在这里选择根域(就是一个系统的基本域)是一个关键，根域名字的选择可以有以下几种方案：

(1) 可以使用一个已经注册的 DNS 域名作为活动目录的根域名，这样的好处在于企业

的公共网络和私有网络使用同样的 DNS 名字。

(2) 还可使用一个已经注册的 DNS 域名的子域名作为活动目录的根域名。

(3) 为活动目录选择一个与已经注册的 DNS 域名完全不同的域名。这样可以使企业网络在内部和互联网上呈现出两种完全不同的命名结构。

(4) 把网络的公共部分用一个已经注册的 DNS 域名进行命名，而私有网络用另一个内部域名，从名字空间上把两部分分开，这样做就使得每一部分要访问另一部分时必须使用对方的名字空间来标识对象。

然后，要进行域和帐户命名规划，因为使用活动目录的意义之一就在于使内、外部网络使用统一的目录服务，采用统一的命名方案，以方便网络管理。

最后，要注意设置规划好域间的信任关系，对于服务端计算机，通过基于 Kerberos V5 安全协议的双向、可传递信任关系启用域之间的帐户验证。

5.2.2　安装、配置活动目录

本节以安装活动目录、配置 test.edu.cn 域为例，在例内建立名称分别为 Win2008sv1 和 Win2008sv2 的两台域控制器。

1. 建立 Win2008sv1 域控制器

建立域林的第一个根域，在名为 Win2008sv1 的计算机上安装第一个域控制器。操作步骤如下：

(1) 以系统管理员帐号如 administrator 登录 Win2008sv1 计算机，并设置其 TCP/IP 属性如下：

- IP 地址：192.168.1.1；
- 子网掩码：255.255.255.0；
- 网关：192.168.1.1(Win2008sv1 的 IP 地址)；
- DNS 服务器的 IP 地址：192.168.1.1(Win2008sv1 的 IP 地址)。

选择“开始”→“管理工具”→“服务器管理器”命令，如图 5-5 所示。

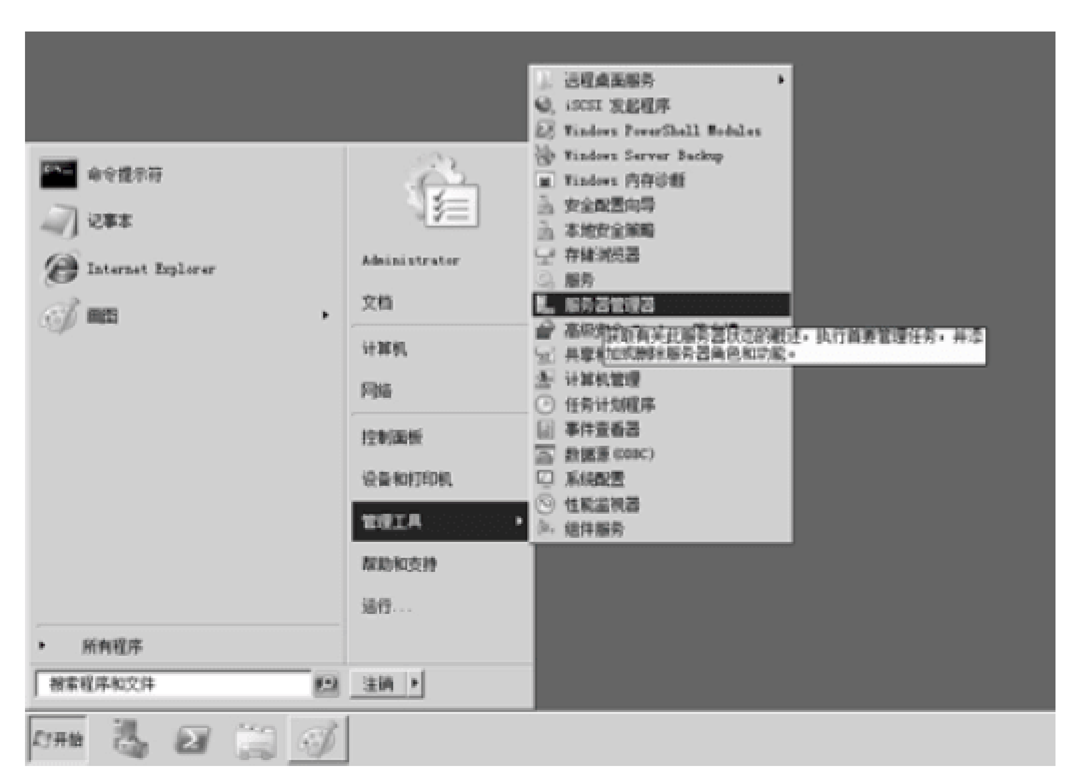


图 5-5　服务器管理器

(2) 在“服务器管理器”管理界面的右边窗格，单击“添加角色”链接，如图 5-6 所示。



图 5-6　服务器管理器

(3) 在“添加角色向导”对话框的“开始之前”界面中，单击“下一步”按钮，如图 5-7 所示。

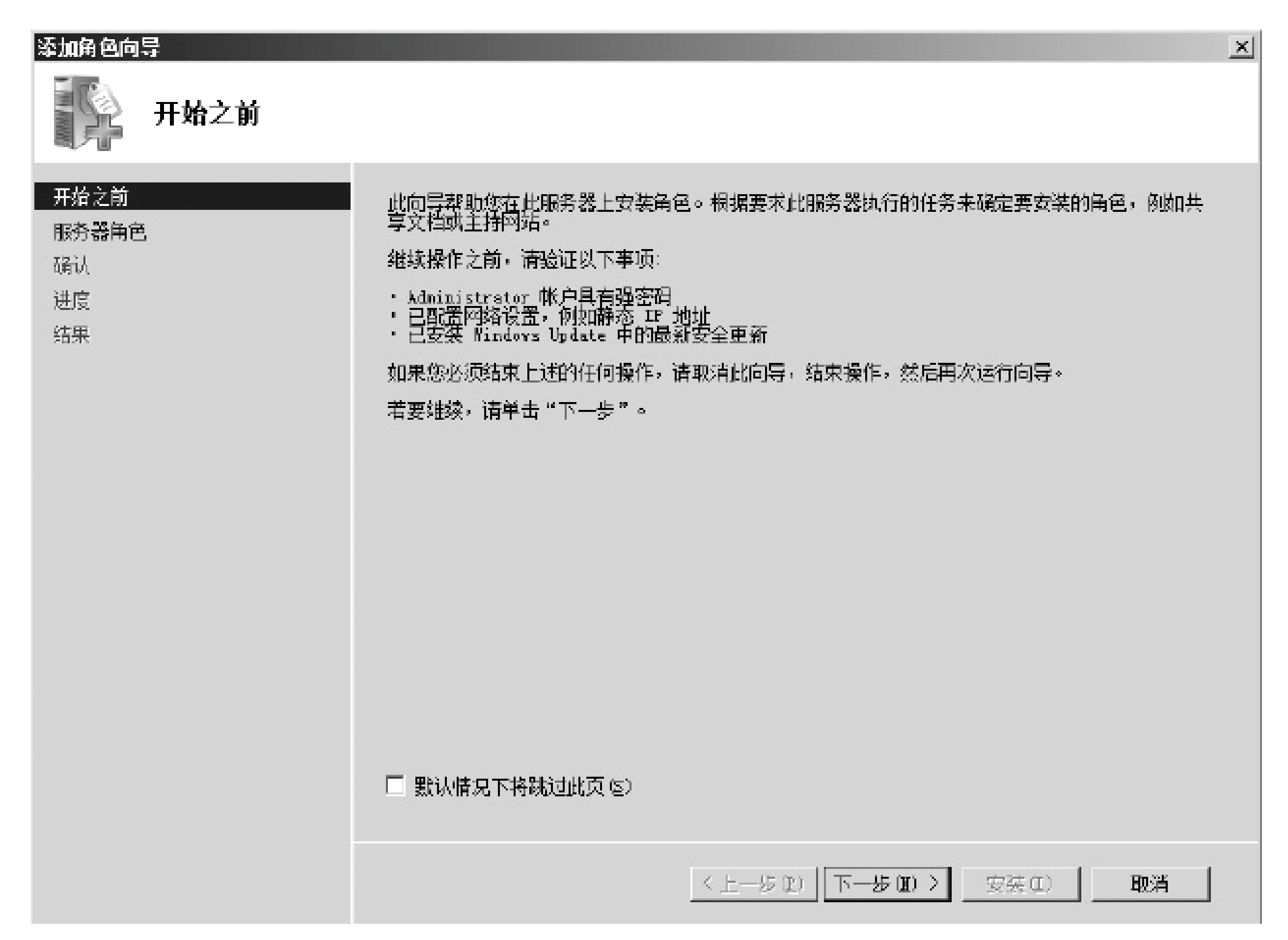


图 5-7　添加角色向导

(4) 在“添加角色向导”对话框的“选择服务器角色”界面中，选中“Active Directory 域服务”复选框，然后单击“下一步”按钮，图 5-8 所示。



图 5-8　选择服务器角色

(5) 在“添加角色向导”对话框的“Active Directory 域服务”界面中，阅读相关信息，然后单击“下一步”按钮，如图 5-9 所示。

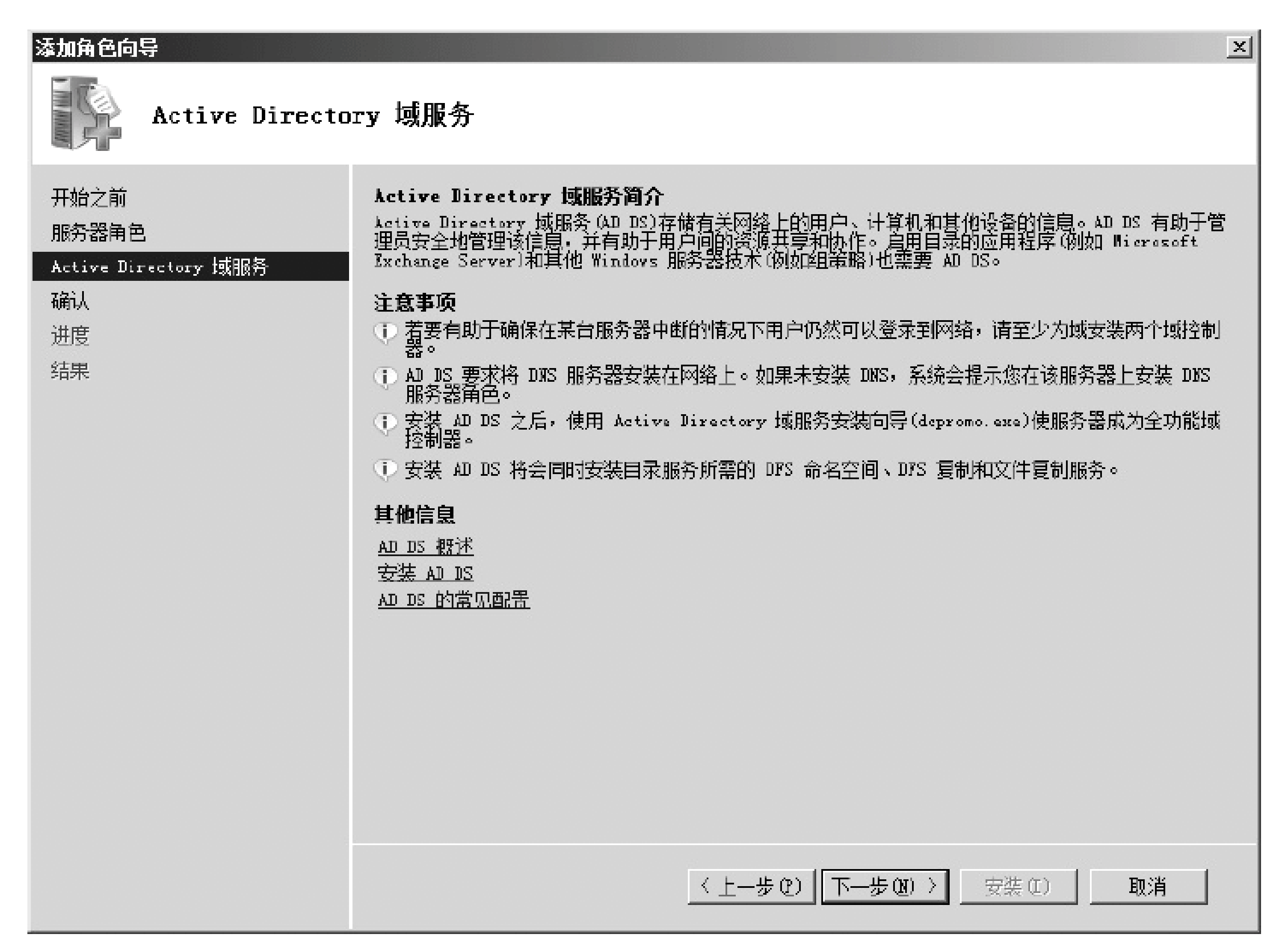


图 5-9　Active Directory 域服务

(6) 在“添加角色向导”对话框的“确认安装选择”界面中，单击“安装”按钮，如图 5-10 所示。

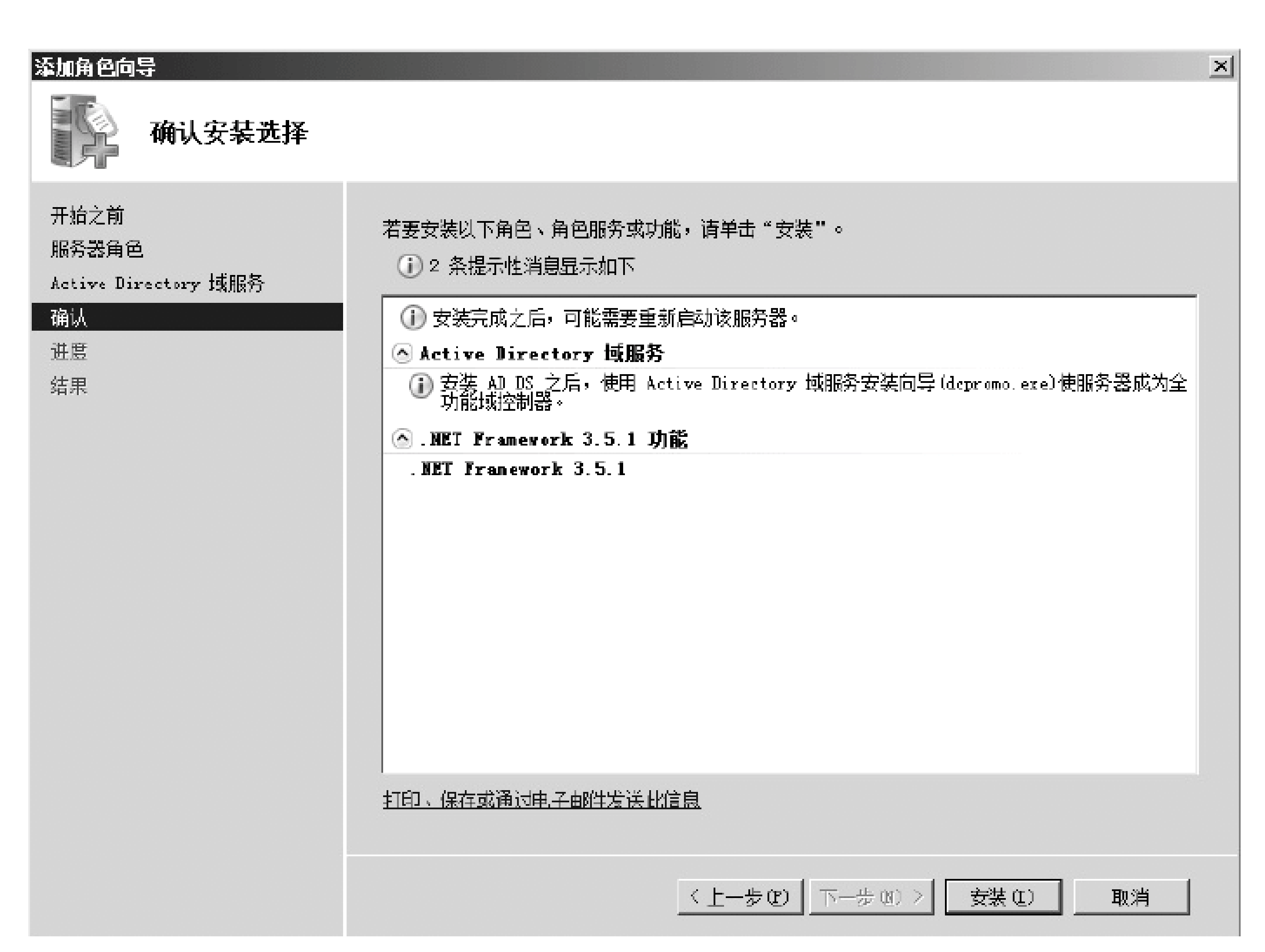


图 5-10　确认安装选择

(7) 在“添加角色向导”对话框的“安装结果”界面中，可以看到显示“安装成功”的字样，代表“Active Directory 域服务”安装成功，单击如图 5-11 所示界面中的“关闭该向导并启动 Active Directory 域服务安装向导(dcpromo.exe)”链接，以启动“Active Directory

域服务安装向导”。

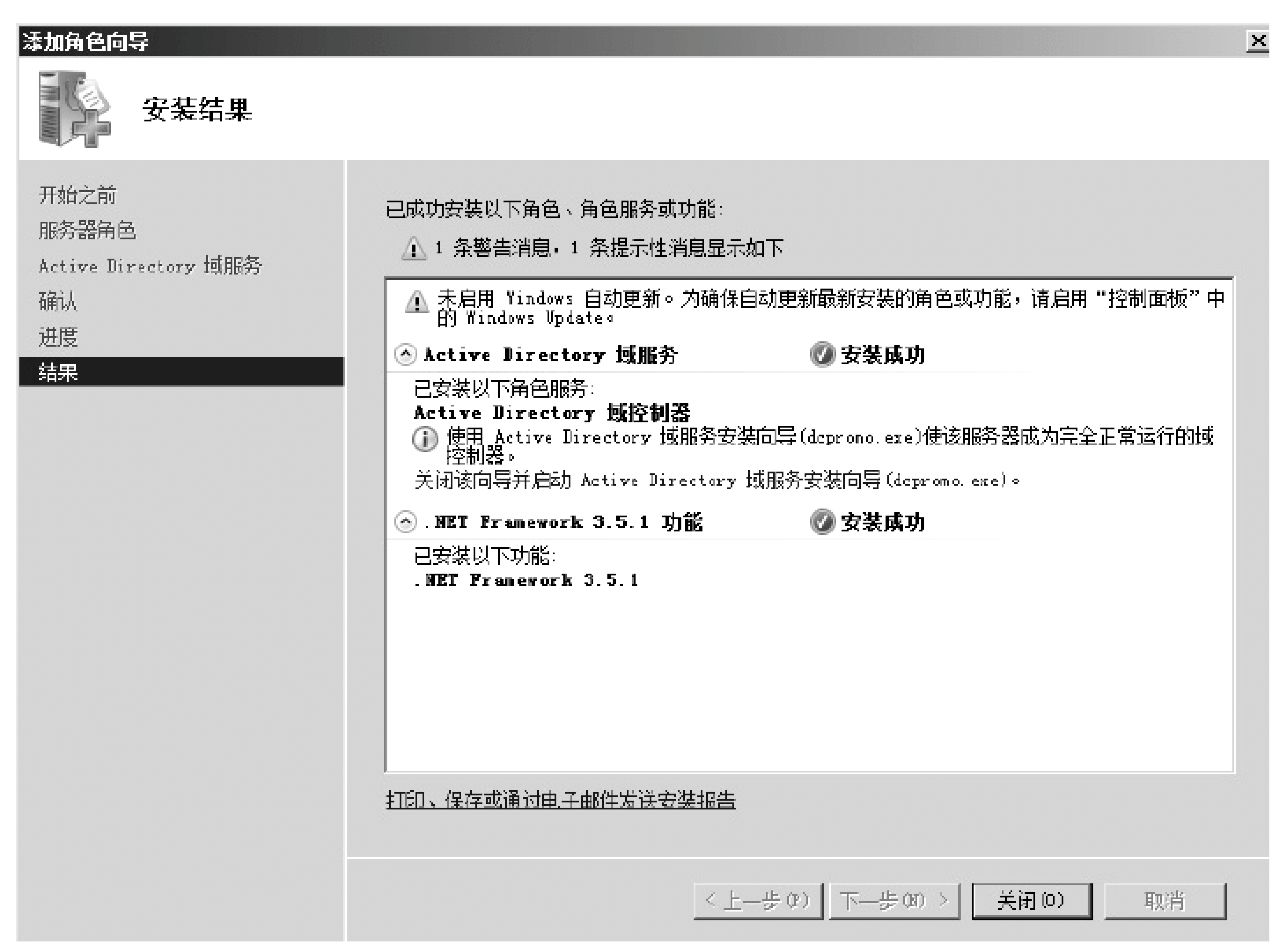


图 5-11 安装结果

(8) 在“Active Directory 域服务安装向导”对话框的“欢迎使用 Active Directory 域服务安装向导”界面，选中“使用高级模式安装”复选框，然后单击“下一步”按钮，如图 5-12 所示。

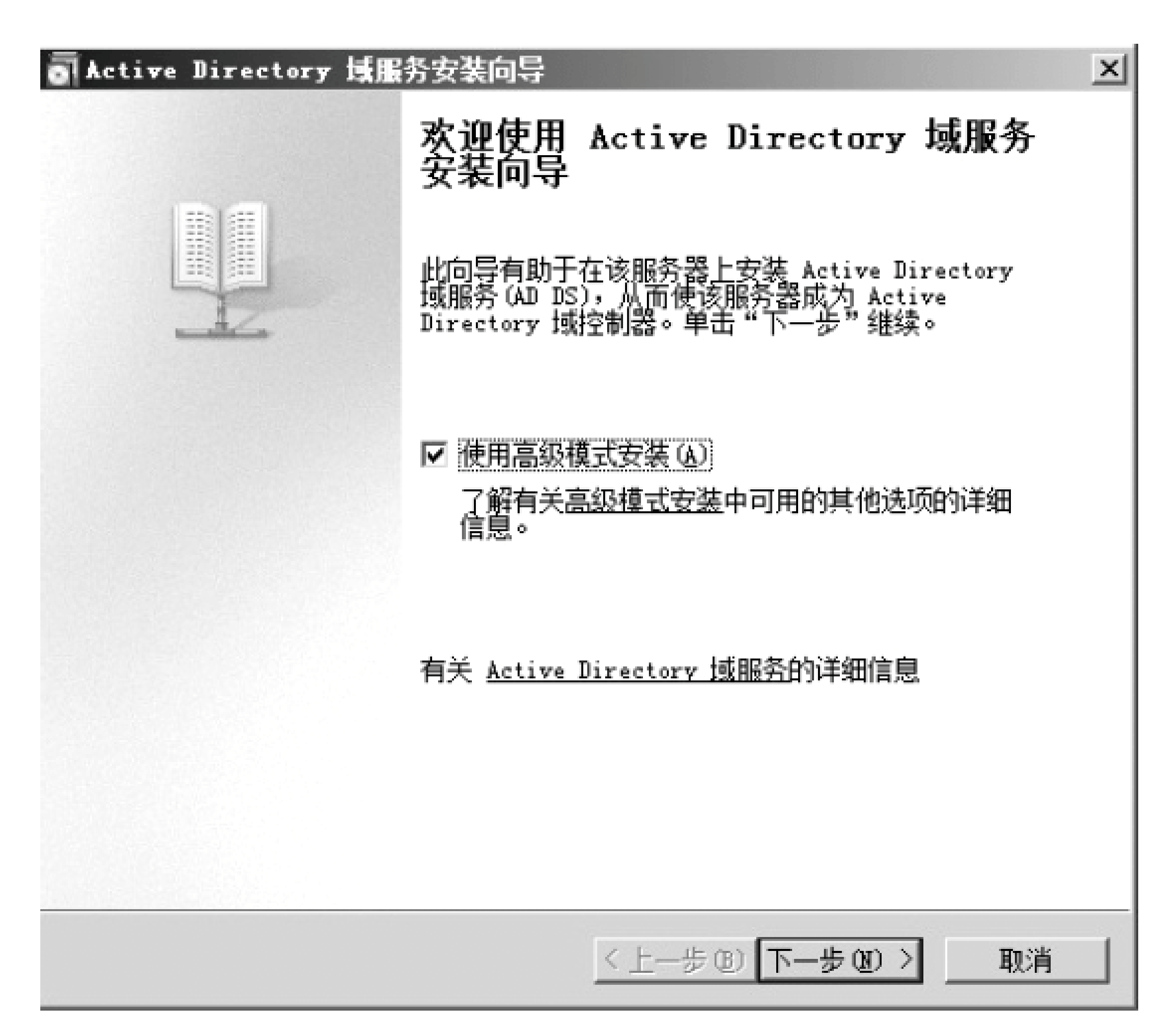


图 5-12 Active Directory 域服务安装向导

(9) 在“Active Directory 域服务安装向导”对话框的“操作系统兼容性”界面中，查看相关信息，然后单击“下一步”按钮，如图 5-13 所示。

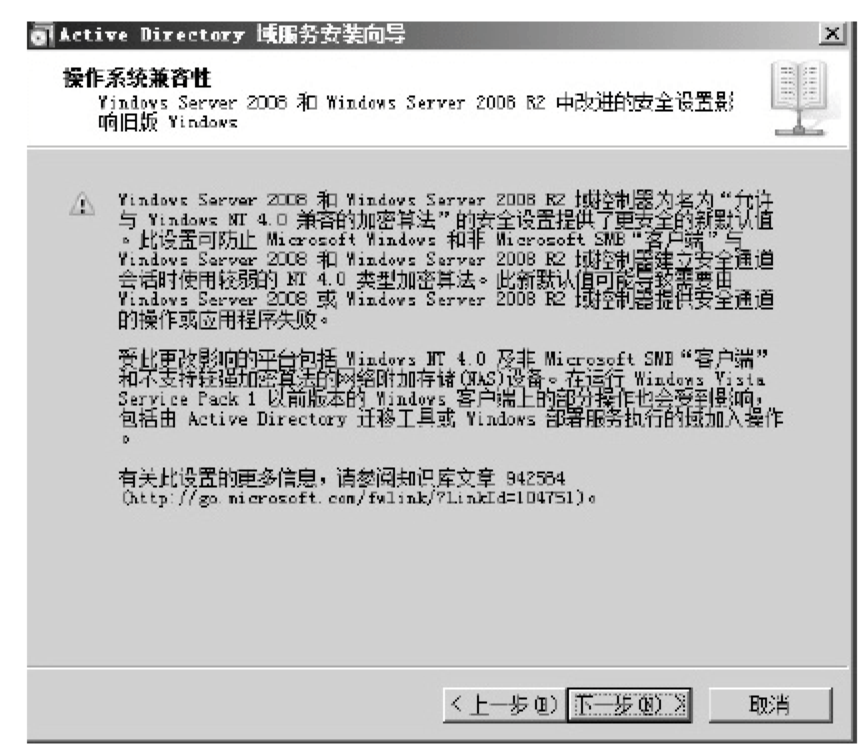


图 5-13　操作系统兼容性

(10) 在“Active Directory 域服务安装向导”对话框的“选择某一部署配置”界面中，选中“在新林中新建域”单选按钮，然后单击“下一步”按钮，如图 5-14 所示。



图 5-14　选择某一部署配置

(11) 在“Active Directory 域服务安装向导”对话框的“命名林根域”界面的“目录林根级域的 FQDN”文本框中，输入要建立的林根域的域名，这里输入 test.edu.cn，然后单击“下一步”按钮，如图 5-15 所示。



图 5-15　设置目录林根级域的 FQDN

(12) 在确认所输入的林根域的 FQDN 与计算机的 NetBIOS 没有冲突后，接着切换至“Active Directory 域服务安装向导”对话框的“域 NetBIOS 名称”界面，在“域 NetBIOS 名称”文本框中确认所输入的 FQDN 名称中最左边的域名，本例为 TEST，然后单击“下一步”按钮，如图 5-16 所示。

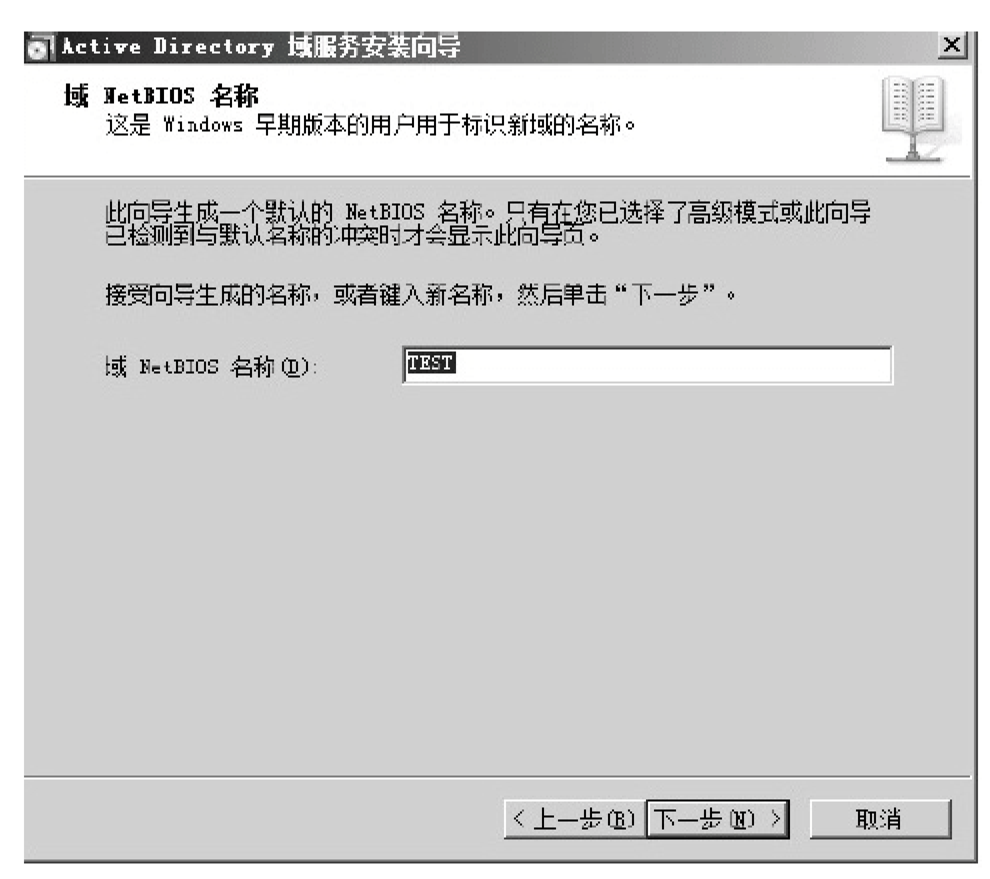


图 5-16　域 NetBIOS 名称

(13) 在“Active Directory 域服务安装向导”对话框的“设置林功能级别”界面的“林功能级别”下拉列表中选择“Windows 2000”选项，然后单击“下一步”按钮，如图 5-17 所示。



图 5-17　设置林功能级别

(14) 在“Active Directory 域服务安装向导”对话框的“设置域功能级别”界面的“域功能级别”下拉列表框中选择“Windows 2000 纯模式”选项，然后单击“下一步”按钮，如图 5-18 所示。



图 5-18　设置域功能级别

(15) 在“Active Directory 域服务安装向导”对话框的“其他域控制器选项”界面中，如图 5-19 所示，确定“DNS 服务器”复选框是被选中的。因为所安装的域控制器是林下的第一台，所以“全局编录”复选框会被强制选中，而“只读域控制器(RODC)”复选框无法选中，主要是因为林中的根域尚未建立，然后单击“下一步”按钮，如果安装向导显示无法建立 DNS 服务器的委派，则单击“是”按钮，以进行手动委派。



图 5-19　其他域控制选项

(16) 在“Active Directory 域服务安装向导”对话框的“数据库、日志文件及 SYSVOL 的位置”界面中，设置数据库、日志文件及 SYSVOL 文件夹的正确路径。本例使用默认值，单击“下一步”按钮，如图 5-20 所示。

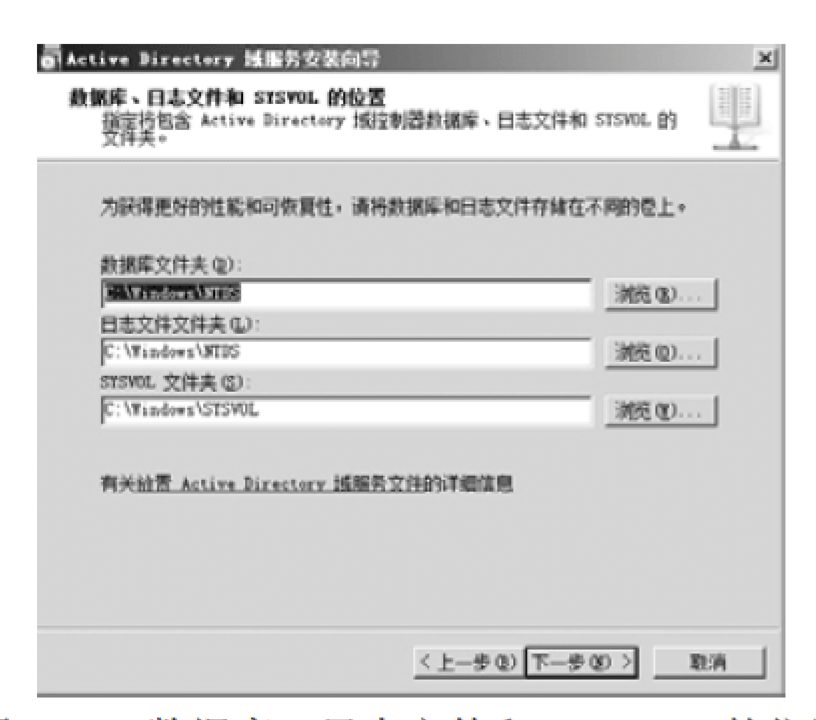


图 5-20　数据库、日志文件和 SYSVOL 的位置

(17) 在“Active Directory 域服务安装向导”对话框的“目录服务还原模式的 Administrator 密码”界面中，设置登录目录服务还原模式时管理员需要输入的密码，然后单击“下一步”按钮，如图 5-21 所示。

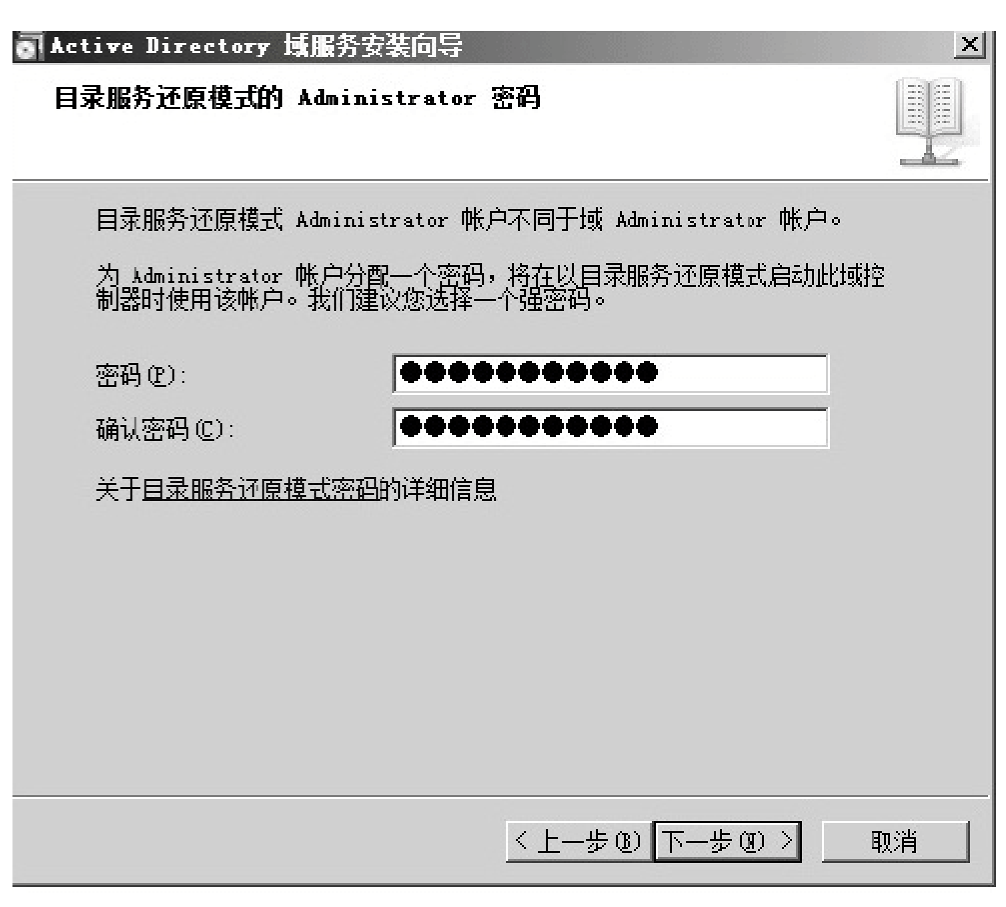


图 5-21　设置 Administrator 密码

(18) 在“Active Directory 域服务安装向导”对话框的“摘要”界面的“检查您的选择”列表框中，查看先前的设置，然后单击“导出设置”按钮，将这台即将建立的域控制器的相关设置予以存储，安装后续域控制器时，即可在命令提示符下通过命令与参数的方式执行安装额外的域控制器，之后单击“下一步”按钮开始安装 Active Directory 域服务，如图 5-22 所示。

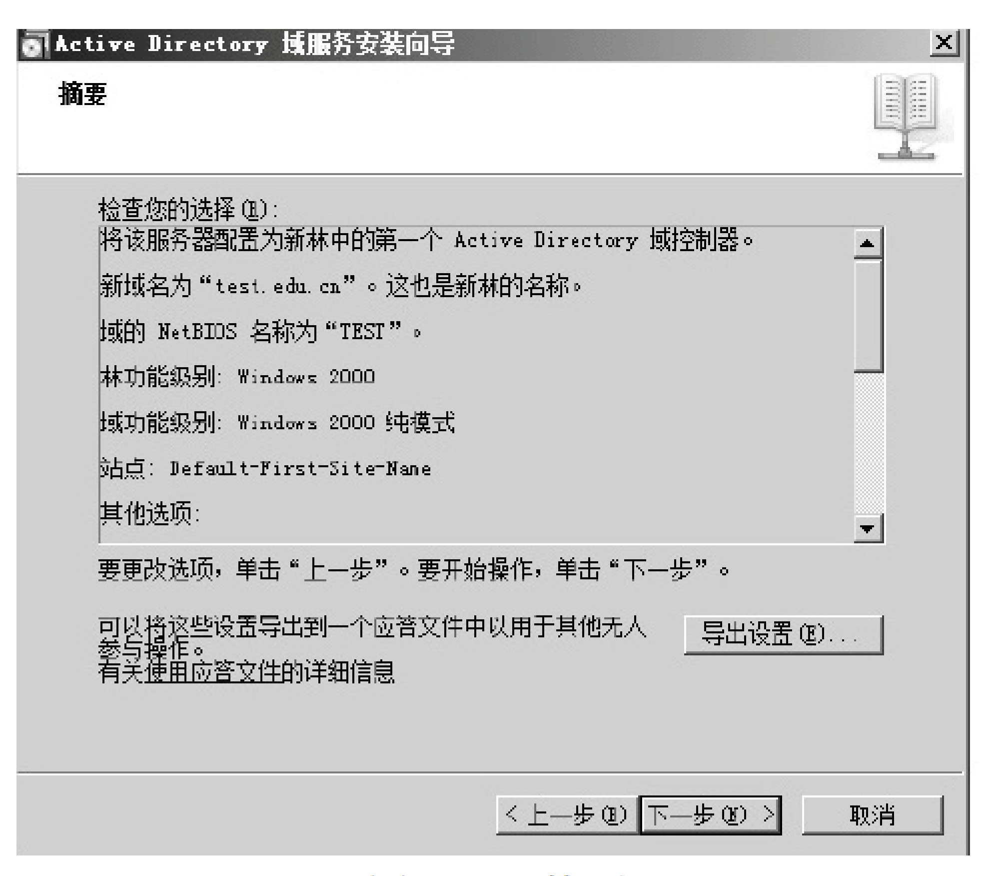


图 5-22　摘要

(19) 在“Active Directory 域服务安装向导”对话框中，显示“完成 Active Directory 域服务安装向导”界面，这代表已经完成 Active Directory 域服务的安装，如图 5-23 所示，单击“完成”按钮，然后单击“立即重新启动”按钮重新启动，以完成林根域的第一台域控制器的安装。



图 5-23　安装完成

通过上述步骤，在名为 Win2008sv1 的计算机上，完成了安装全新林中根域的域控制器。

2. 建立额外的域控制器

在 Win2008sv2 计算机上为 test.edu.cn 域建立额外的域控制器，与建立林根域中第一台域控制器的过程非常类似，步骤如下：

(1) 以系统管理员帐号如 administrator 登录 Win2008sv2 计算机，并设置其 TCP/IP 属性。

- IP 地址：192.168.1.2；
- 子网掩码：255.255.255.0；
- 网关：192.168.1.1(Win2008sv1 的 IP 地址)；
- DNS 服务器的 IP 地址：192.168.1.1(Win2008sv1 的 IP 地址)。

(2) 参考上述方法建立第一台域控制器中的步骤(2)~(10)的操作。

(3) 在“Active Directory 域服务安装向导”对话框的“选择某一部署配置”界面中，选中“现有林”单选按钮，再选中“向现有域添加域控制器”单选按钮，然后单击“下一步”按钮，如图 5-24 所示。

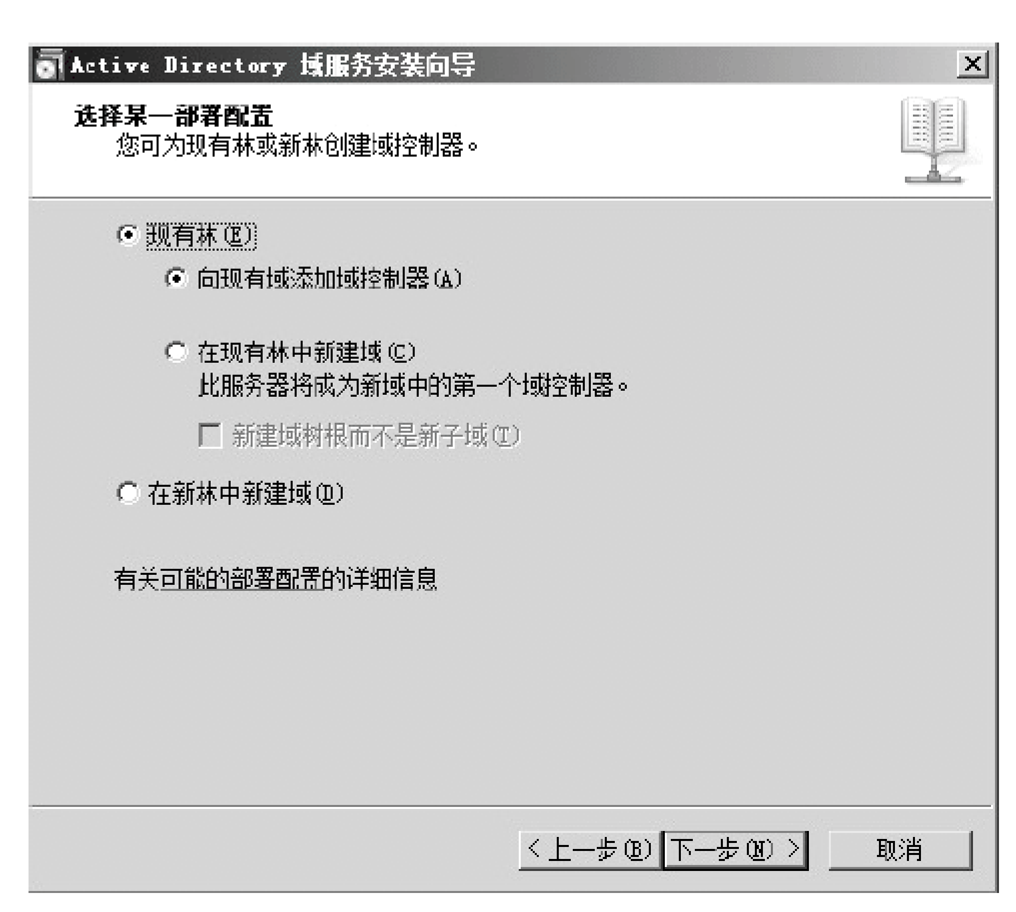


图 5-24　选中“现有林”单选按钮

(4) 在“Active Directory 域服务安装向导”对话框的“网络凭据”界面，输入 Administrator 与其密码，如图 5-25 所示，然后单击“确定”按钮，再单击“下一步”按钮。



图 5-25　Windows 安全

(5) 在“Active Directory 域服务安装向导”对话框的“选择域”界面的“域”列表框中选择“test.edu.cn(林根域)”选项，然后单击“下一步”按钮，如图 5-26 所示。



图 5-26　选择域

(6) 在“Active Directory 域服务安装向导”对话框的“请选择一个站点”界面的“站点”列表框中选择“Default-First-Site-Name”选项，然后单击“下一步”按钮，如图 5-27 所示。



图 5-27　选择一个站点

(7) 在“Active Directory 域服务安装向导”对话框的“其他域控制器选项”界面中，取消选中“DNS 服务器”与“全局编录”复选框，如图 5-28 所示。实际上，如果考虑到 DNS 服务器与全局编录服务器的容错与效率因素，也可以考虑将它们选中。而“只读域控制器(RODC)”复选框无法选中，是因为安装条件不符合。单击“下一步”按钮。

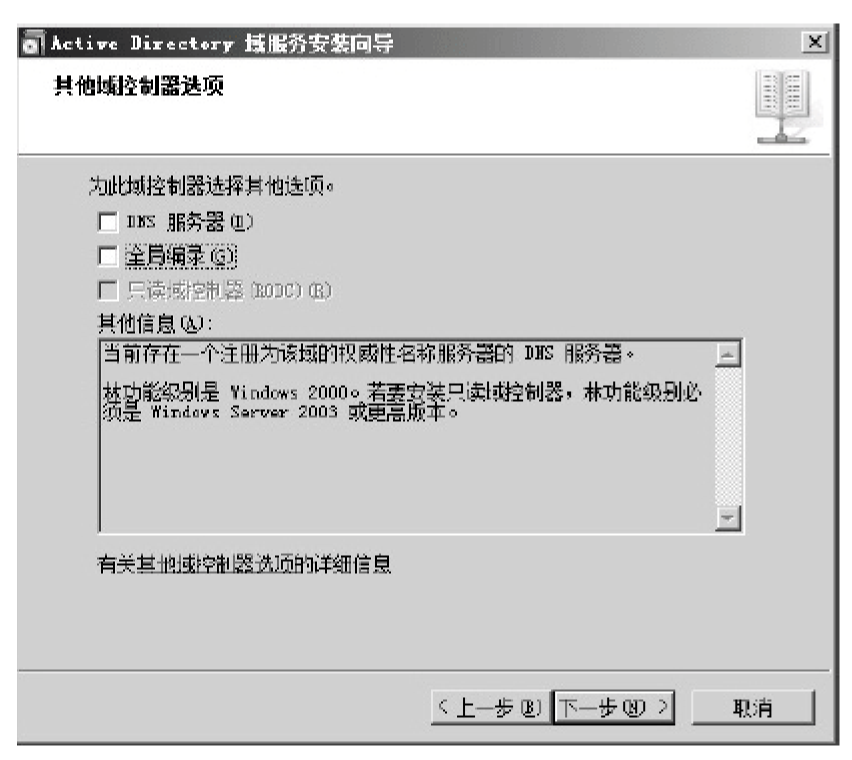


图 5-28　其他域控制器选项

(8) 在“结构主机配置冲突”对话框中，选择“将结构主机角色传送到此域控制器”选项，如图 5-29 所示。

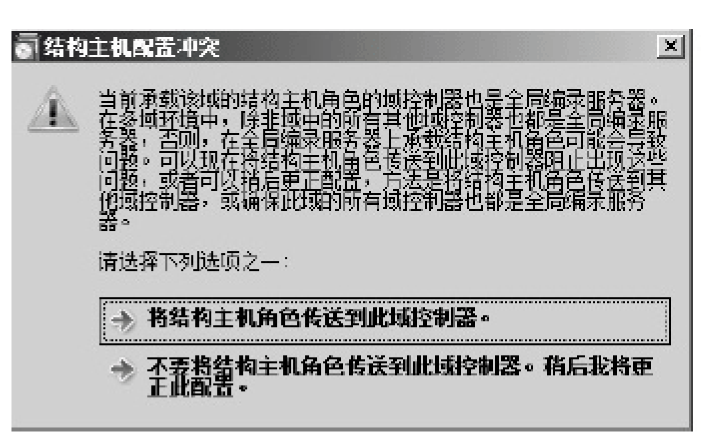


图 5-29　结构主机配置冲突

(9) 在“Active Directory 域服务安装向导”对话框的“从介质安装”界面中，选中“通过网络从现有域控制器复制数据”单选按钮。让安装向导通过网络复制现有域控制器的 AD DS 数据库中的数据时可以降低复制的流量。单击“下一步”按钮，如图 5-30 所示。

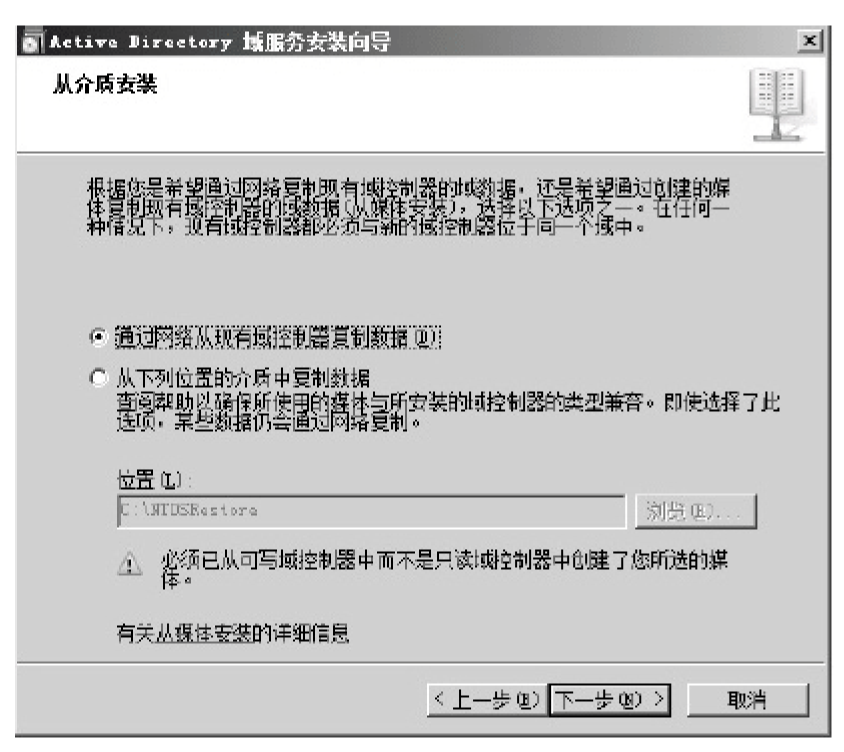


图 5-30　从介质安装

(10) 在“Active Directory 域服务安装向导”对话框“源域控制器”界面的“为安装伙伴选择源域控制器”选项组中选中“让向导选择一个合适的域控制器”单选按钮，然后单击“下一步”按钮，如图 5-31 所示。

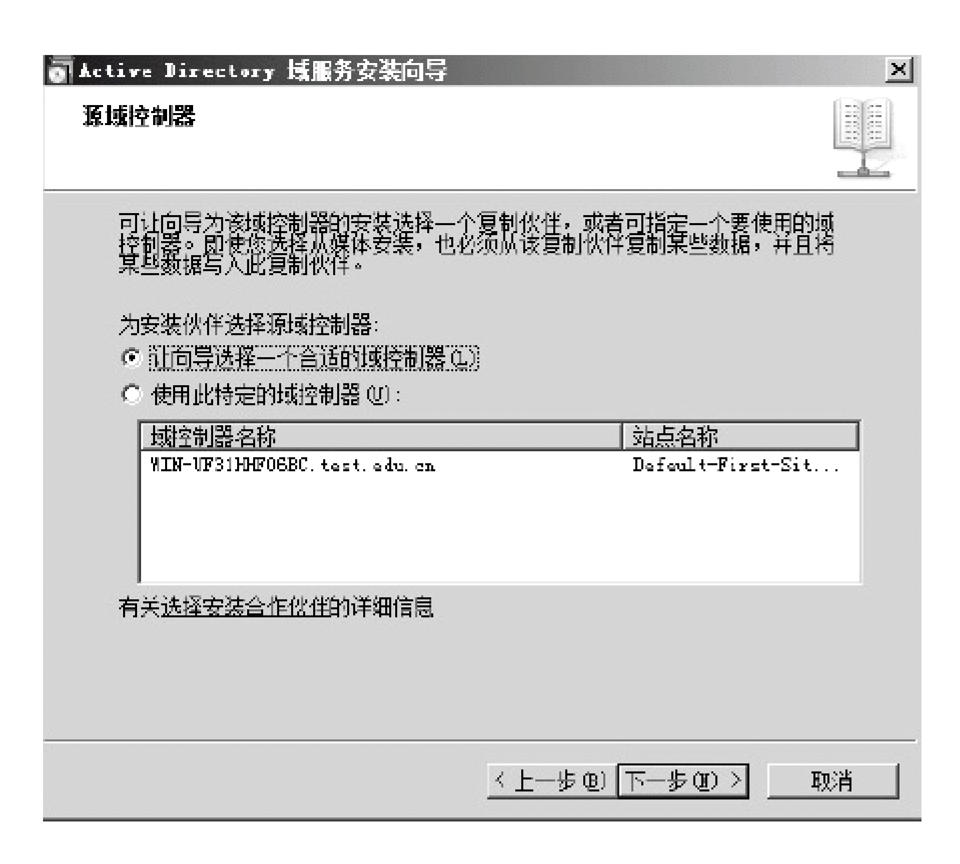


图 5-31　选择合适域控制器

(11) 接下来的步骤参考之前的安装第一台域控制器中的第(1)～(19)步的操作。

(12) 在“Active Directory 域服务安装向导”对话框显示如图 5-32 所示的界面，说明正在安装第二台域控制器，需要通过网络与 test.edu.cn 域中的现存域控制器进行 AD DS 数据库的复制。



图 5-32　向导正在配置 Active Directory 域服务

(13) 在“Active Directory 域服务安装向导”对话框中显示“正在完成 Active Directory 域服务安装向导”界面，这代表已经完成 Active Directory 域服务的安装，单击“完成”按钮，然后单击“立即重新启动”按钮重新启动，以完成第二台域控制器的安装。

完成上述操作步骤后，test.edu.cn 域内已经有了 Win2008sv1 和 Win2008sv2 两台域控制器，如图 5-33 所示。这两个区域控制器可同时提供域用户登录域时身份验证的工作。此外，这两台域控制器都有一个可读写入的 AD DS 数据库，它们会自动执行 AD DS 数据库复制工作，以便维持目录服务数据库的一致性。

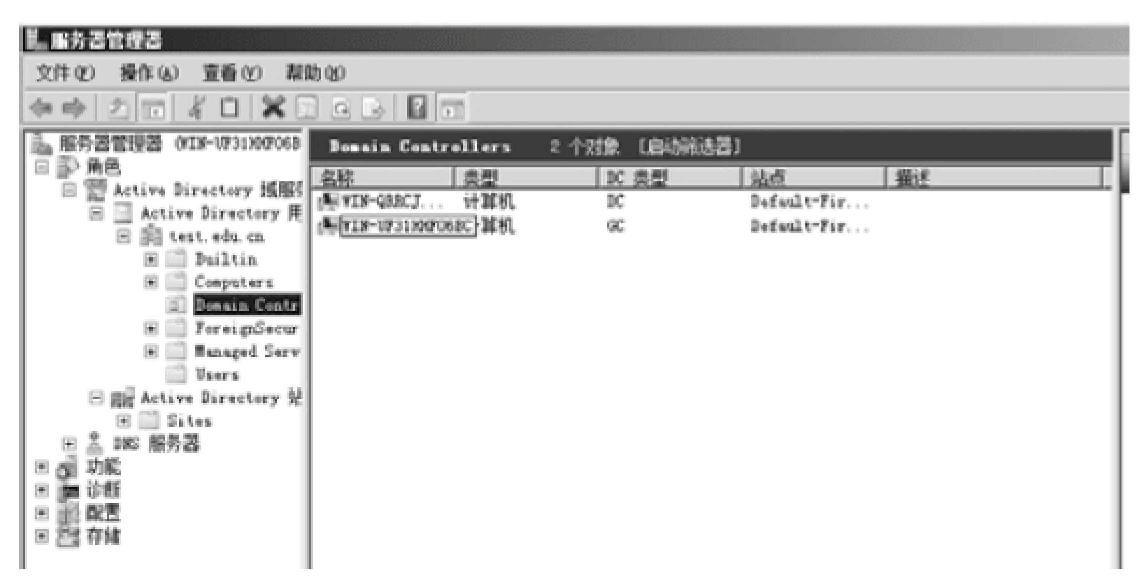


图 5-33　配置完成

5.2.3　删除活动目录与域

将活动目录从域控制器删除之前需要注意以下事项：

(1) 如果域内还有其他域控制器存在，则降级后这台机器会成为该域的成员服务器，其计算机帐户会被从组织单元域控制器转移到容器 computers 内。只有 Domain Admins 或 Enterprise Admins 组内的成员才有权限删除域控制器。

(2) 如果这台域控制器是域内的最后一台域控制器，则删除域控制器，同时 test.edu.cn 域也会被删除，这台机器降级后会变成一台独立服务器或者是工作组服务器。只有 Enterprise Admins 组内的用户才能有权限删除最后一个域控制器，而且如果有子域的话，应该先删除子域。

(3) 如果删除的是林内的最后一台域控制器，那么删除域控制器之后林同时也被删除。只有 Enterprise Admins 组内的用户才有权限删除。

(4) 如果这台服务器是全局编录服务器(GC)，则要检查其所属的站点是否还有其他的 GC，若没有，需要指定一台域控制器作为 GC。依次单击“开始”→“管理工具”→“Active Directory 站点和服务”→“站点”→“default-first-site-name”→“服务器”，选择要扮演 GC 的服务器，右击“NTDS 设置”，从弹出的快捷菜单选择“属性”命令，然后选择“全局编录”。

需要注意，删除活动目录、脱离域是影响服务器作用的首要方法，如图 5-34 所示。

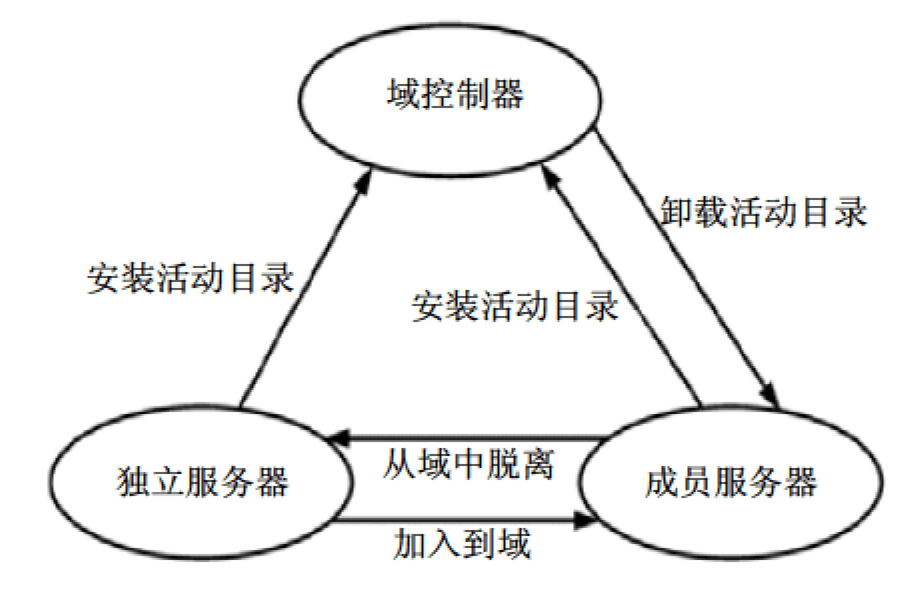


图 5-34　删除活动目录、脱离域对服务器作用的影响

安装好的域控制器的角色是可以更改的，可从域控制器上删除 Active Directory，使其

作用降级，其中，删除域中最后一个域控制器的步骤如下：

(1) 依次单击“开始”→“运行”，在打开的“运行”对话框输入 dcpromo，然后按 Enter 键。

(2) 在“欢迎使用 Active Directory 域服务安装向导”界面上，单击“下一步”按钮。

(3) 在“删除域”界面上，如图 5-35 所示，选择包含“删除该域”字样的选项。继续之前，如果必要，先阅读有关管理删除加密密钥和解密使用加密文件系统(EFS)加密的文件说明，然后再执行这些操作。确保完成了所有安全任务之后，单击“下一步”按钮。

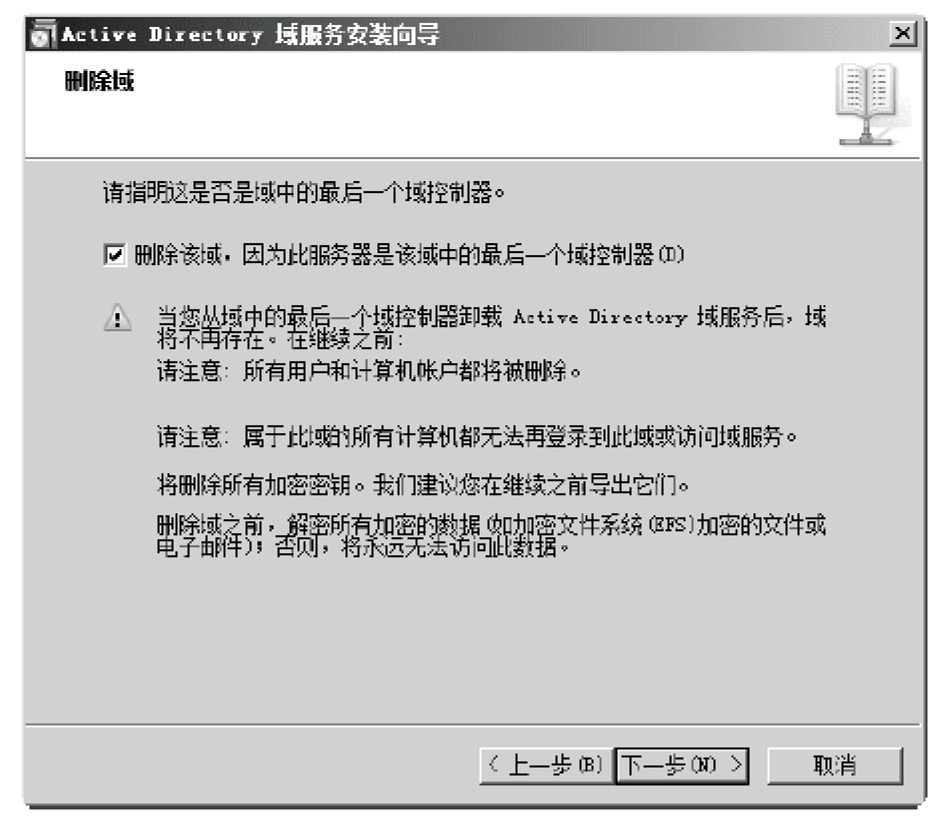


图 5-35　删除活动目录

(4) 如果该域控制器具有应用程序目录分区，则在“应用程序目录分区”界面上，查看列表中的应用程序目录分区，然后按照如下方式删除或保留应用程序目录分区：

- 如果不想保留存储在域控制器上的任何应用程序目录分区，单击“下一步”按钮。
- 如果想保留某个应用程序已经在域控制器上创建的任何应用程序目录分区，则使用创建该分区的应用程序将其移除到另一个域控制器，然后单击“更新列表”以更新列表。

(5) 在“确认删除”界面上，选择删除域控制器上所有应用程序目录分区的选项，然后单击“下一步”按钮。

(6) 在“删除 DNS 委派”界面上，确认选中了“删除指向此服务器的 DNS 委派”复选框，然后单击“下一步”按钮。

(7) 如有必要，为承载 DNS 区域(其中包含服务器的 DNS 委派)的服务器输入管理凭据，然后单击“确定”按钮。

(8) 在“网络凭据”界面上，按实际需要进行操作。

- 如果当前以 Enterprise Admins 成员的身份登录，则单击“下一步”按钮。
- 如果使用另一个帐户登录，则单击“备用凭据”，单击“设置”，输入 Enterprise Admins 组成员的帐户名称和密码，然后单击“下一步”按钮。

(9) 在“管理员密码”界面上，为本地 Administrator 帐户输入安全密码并确认，然后单击“下一步”按钮。

(10) 在“摘要”界面上，若要将所选择的设置保存到可用来自动执行以后的活动目录操作的答案文件，则单击“导出设置”，输入答案文件名，然后单击“保存”按钮。查看选择，然后单击“下一步”按钮以删除活动目录。

(11) 在“完成 Active Directory 域服务安装向导”界面上，单击“完成”按钮。

(12) 然后，系统提示是否重新启动操作系统。选择重新启动服务器，以完成对活动目录的删除。

5.3　用户与组的管理

通过建立域控制器实现目录管理(即活动目录)，计算机加入域成为活动目录中的一个计算机帐户，但如要获得活动目录中的资源，还必须在活动目录数据库中创建用户帐户，同时为帐户设置一个安全的密码。用户帐户是计算机的基本安全手段，计算机通过用户帐户来辨别用户身份，让有使用权限的人登录计算机，访问本地计算机资源或从网络访问这台计算机的共享资源。

Windows Server 2008 支持以下两种用户帐户：域帐户和本地帐户。

域帐户可以登录到域上，并获得访问该网络的权限；本地帐户则只能登录到一台特定的计算机上，并访问该计算机上的资源。Windows Server 2008 还提供内置用户帐户，它用于执行特定的管理任务或使用户能够访问网络资源。

本地用户帐户仅允许用户登录并访问创建该帐户的计算机。在创建本地用户帐户时，Windows Server 2008 仅在计算机位于%Systemroot%\system32\config 文件夹下的安全数据库(SAM)中创建该帐户。

Windows Server 2008 默认只有 Administrator 帐户和 Guest 帐户。Administrator 帐户可以执行计算机管理的所有操作；而 Guest 帐户是为临时访问计算机的用户而设置的，但默认是禁用的。

用户登录后，可以在命令提示符状态下输入“whoami /logonid”命令查询当前用户帐户的安全标识符，如图 5-36 所示。



图 5-36　查询当前用户帐户的安全标识符

系统的内置帐户 Administrator 和 Guest 的功能权限如下。

- Administrator：使用内置 Administrator 帐户可以对整台计算机或域配置进行管理，如创建修改用户帐户和组、管理安全策略、创建打印机、分配允许用户访问资源的权限等。作为管理员，应该创建一个普通用户帐户，在执行非管理任务时使用该用

户帐户，仅在执行管理任务时才使用 Administrator 帐户。Administrator 帐户可以更名，但不可以删除。

- Guest：一般的临时用户可以使用内置 Guest 帐户进行登录并访问资源。在默认情况下，为了保证系统的安全，Guest 帐户是禁用的，但在安全性要求不高的网络环境中，可以使用该帐户，且通常给它分配一个口令。

遵循以下的规则和约定可以简化帐户创建后的管理工作。

(1) 命名约定

① 帐户名必须唯一：本地帐户必须在本地计算机上唯一。

② 帐户名不能包含以下字符：* / \ [ ] : ; | = ， + / < >"。

③ 帐户名最长不能超过 20 个字符。

(2) 密码原则

① 一定要给 Administrator 帐户指定一个复杂的密码，以防止他人随便使用该帐户。

② 确定是管理员还是用户拥有密码的控制权。用户可以给每个用户帐户指定一个唯一的密码，并防止他用户对其进行更改，也可以允许用户在第一次登录时输入自己的密码。一般情况下，用户应该可以控制自己的密码。

③ 密码最多可由 128 个字符组成，推荐最小长度为 8 个字符。

④ 密码应由大小写字母、数字以及合法的非字母数字的字符混合组成，如 P@ssw0rd。

组帐户是计算机的基本安全手段，用户帐户的集合。组帐户并不能用于登录计算机，但可以用于组织用户帐户。通过使用组，管理员可以同时向一组用户分配权限，故可简化对用户帐户的管理。

组可以用于组织用户帐户，让用户继承组的权限，如表 5-1 所示。

表 5-1　内置组的帐户的权限

组	描述	默认用户权限
Administrators	该组的成员具有对服务器的完全控制权限，并且可以根据需要向用户指派用户权利和权限。默认成员有 Administrator 帐户	从网络访问此计算机；允许本地登录；调整某个进程的内存配额；允许通过终端服务登录；备份文件和目录；更改系统时间；调试程序；从远程系统强制关机；加载和卸载设备驱动程序；管理审核和安全日志；调整系统性能；关闭系统；取得文件或其他对象的所有权
Backup Operators	该组的成员可以备份和还原服务器上的文件，而不考虑保护这些文件的安全设置。这是因为执行备份的权限优先于所有文件的使用权限，但是不能更改文件的安全设置	从网络访问此计算机；允许本地登录；备份文件和目录；忽略遍历检查；还原文件和目录；关闭系统
Guests	该组成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾帐户(默认情况下禁用)也是该组的默认成员	没有默认用户权限

5.3.1　本地用户和组

1. 本地用户的创建与管理

以管理员帐号如 administrator 登录计算机，可以用“计算机管理”中的“本地用户和组”管理单元来创建本地用户帐户，操作步骤如下：

(1) 右击桌面上的“计算机”图标，选择“管理”→“配置”→“本地用户和组”→“用户”命令，出现如图 5-37 所示的“服务器管理器”窗口。

(2) 展开“配置”、“本地用户和组”，右击“用户”，从弹出的快捷菜单中选择“新用户”命令，如图 5-38 所示。

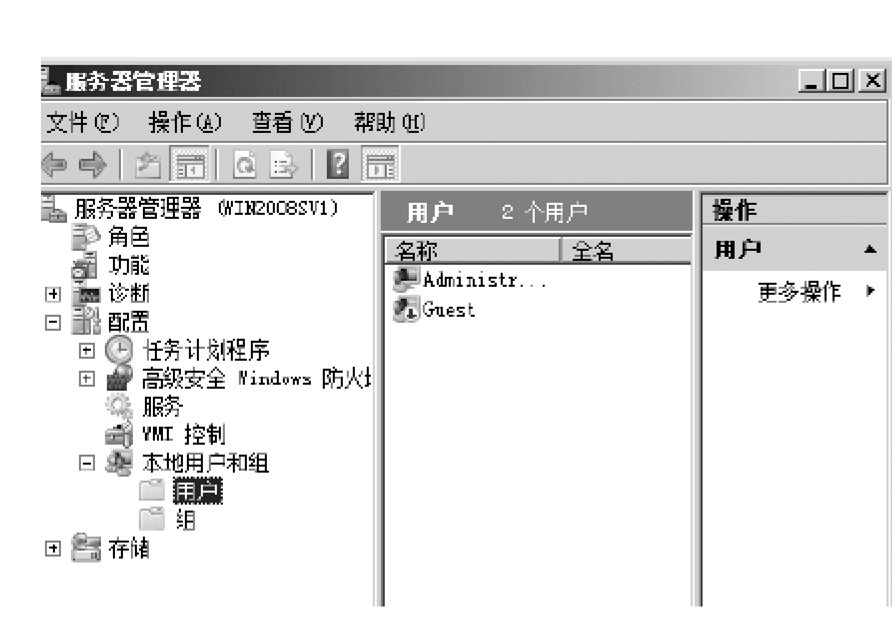


图 5-37　打开“服务器管理器”窗口



图 5-38　右击“用户”

(3) 打开“新用户”对话框后，输入用户名、全名和描述信息，并输入密码，如图 5-39 所示，更改密码文本框下面的 4 个属性的选择状态，然后单击“创建”按钮，返回如图 5-37 所示的窗口。

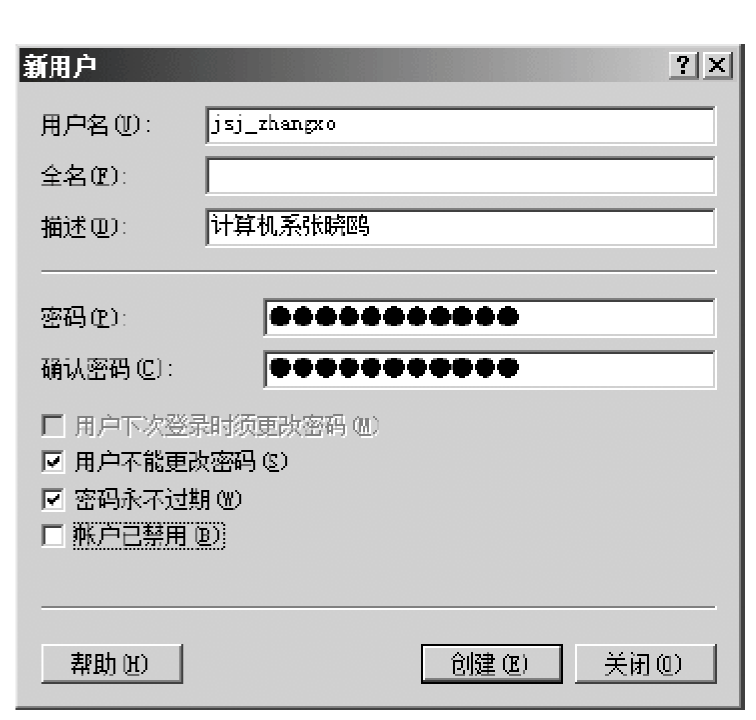


图 5-39　输入用户信息

用户帐户还具有其他的属性，如用户隶属的用户组、用户配置文件、用户的拨入权限、终端用户设置等。在“本地用户和组”的右侧栏中，双击一个用户，将显示该用户的属性对话框，如图 5-40 所示。

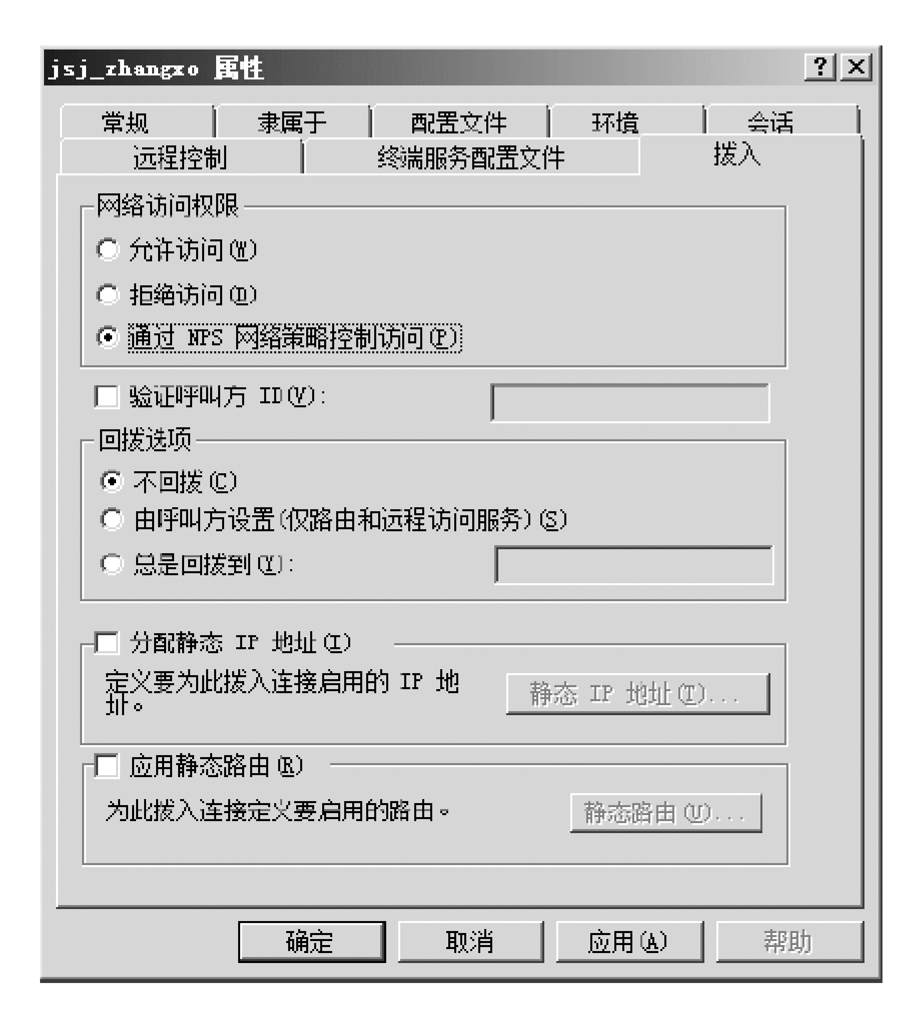


图 5-40　用户的属性对话框

在图 5-41 所示的窗口中，右击任一用户帐户，从弹出的快捷菜单中可重新设置密码、删除、重命名等。

注意：

系统内置帐户如 Administrator、Guest 无法删除。



图 5-41　删除用户帐户

2. 本地组的创建与管理

操作步骤如下：

(1) 单击图 5-37 中的“组”，可以查看本地内置的所有组帐户，如图 5-42 所示，这里将以下将要建立到的非内置组称为“用户组”。



图 5-42　本地内置的所有组帐户

(2) 右击“组”选项，从弹出的快捷菜单中选择“新建组”命令，如图 5-43 所示。



图 5-43　右击“组”

(3) 在“新建组”对话框中输入组名和描述，如图 5-44 所示。若要为该组添加成员用户，依次单击“添加”、“高级”按钮，打开如图 5-45 所示的“选择用户”对话框。

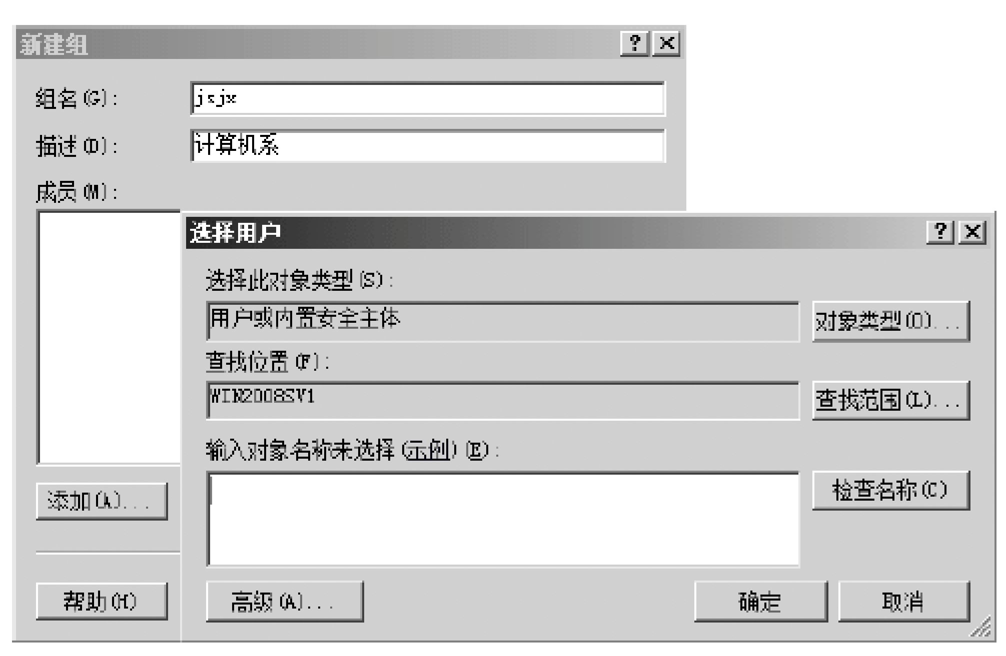


图 5-44　输入组信息

(4) 单击“立即查找”按钮，选择用户名，如 jsj_zhangxo，单击“确定”按钮，返回“选择用户”对话框，如图 5-45 所示。



图 5-45　查找用户名

(5) 在如图 5-46 所示的对话框中单击“确定”按钮，返回“新建组”对话框，如图 5-47 所示。



图 5-46　单击“确定”按钮



图 5-47　完成组的创建

(6) 在“新建组”对话框中单击“创建”按钮，完成组的创建，返回“服务器管理器”窗口。

(7) 在返回“服务器管理器”窗口中，右击任一用户组，利用弹出的快捷菜单，可以

进行删除、重命名、更改属性等管理操作，如图 5-48 所示。每个组都拥有一个唯一的安全标识符(SID)，所以一旦删除了用户组，就不能重新恢复，即使新建一个与被删除组有相同名字和成员的组，也不会与被删除组有相同的特性和特权。



图 5-48　管理用户组

管理员只能删除新增的组，不能删除系统内置的组。当管理员删除系统内置组时，系统将拒绝删除操作。重命名组的操作与删除组的操作类似，只需要在右键弹出菜单中选择“重命名”命令，输入相应的名称后按回车键即可。

当服务器升级为域控制器，则该服务器上的本地帐户被自动转为域用户帐户，因此，在域控制器中不存在本地用户帐户。

5.3.2　域用户帐户

Active Directory 用户帐户和计算机帐户代表物理实体，如人或计算机。用户帐户也可用做某些应用程序的专用服务帐户。用户帐户和计算机帐户以及组也称为安全主体。安全主体是被自动指派了安全标识符(SID)的目录对象。用户或计算机帐户在系统中可以用于以下几个方面：

(1) 验证用户或计算机的身份；

(2) 授权或拒绝访问域资源；

(3) 管理其他安全主体；

(4) 审核使用用户或计算机帐户执行的操作。

组是用户和计算机帐户、联系人以及其他可作为单个单元管理的集合，属于特定组的用户和计算机称为组成员。组都有一个作用域，用来确定在域树或林中该组的应用范围。有 3 种组作用域：通用组、全局组和本地域组。通用组的成员包括域树或林中任何域中的其他组和帐户，而且可在该域树或林中的任何域中指派权限。全局组的成员包括组定义所在域中的其他组和帐户，而且可在林中的任何域中为组的成员帐户指派权限。本地域组的成员可包括 Windows Server 2008、Windows 2000 或 Windows NT 域中的其他组和帐户，而且只能在域内指派权限。通过对 Active Directory 中的组进行管理，可以实现如下功能：简

化管理和委派管理。

1. “Active Directory 用户和计算机”管理控制台简介

域中的用户帐户、组、组织单位等日常的管理工作都是在“Active Directory 用户和计算机”控制台中进行的，因此首先来介绍一下它的基本组成。

选择桌面左下角的“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”(或直接在运行框中输入命令 dsa.msc)，打开如图 5-49 所示的窗口，在左边树形结构窗格中，Windows Server 2008 一旦安装 Active Directory 服务后，默认产生多种容器(当前默认显示在控制台中有 5 种)，不同容器保存着不同类型的对象。

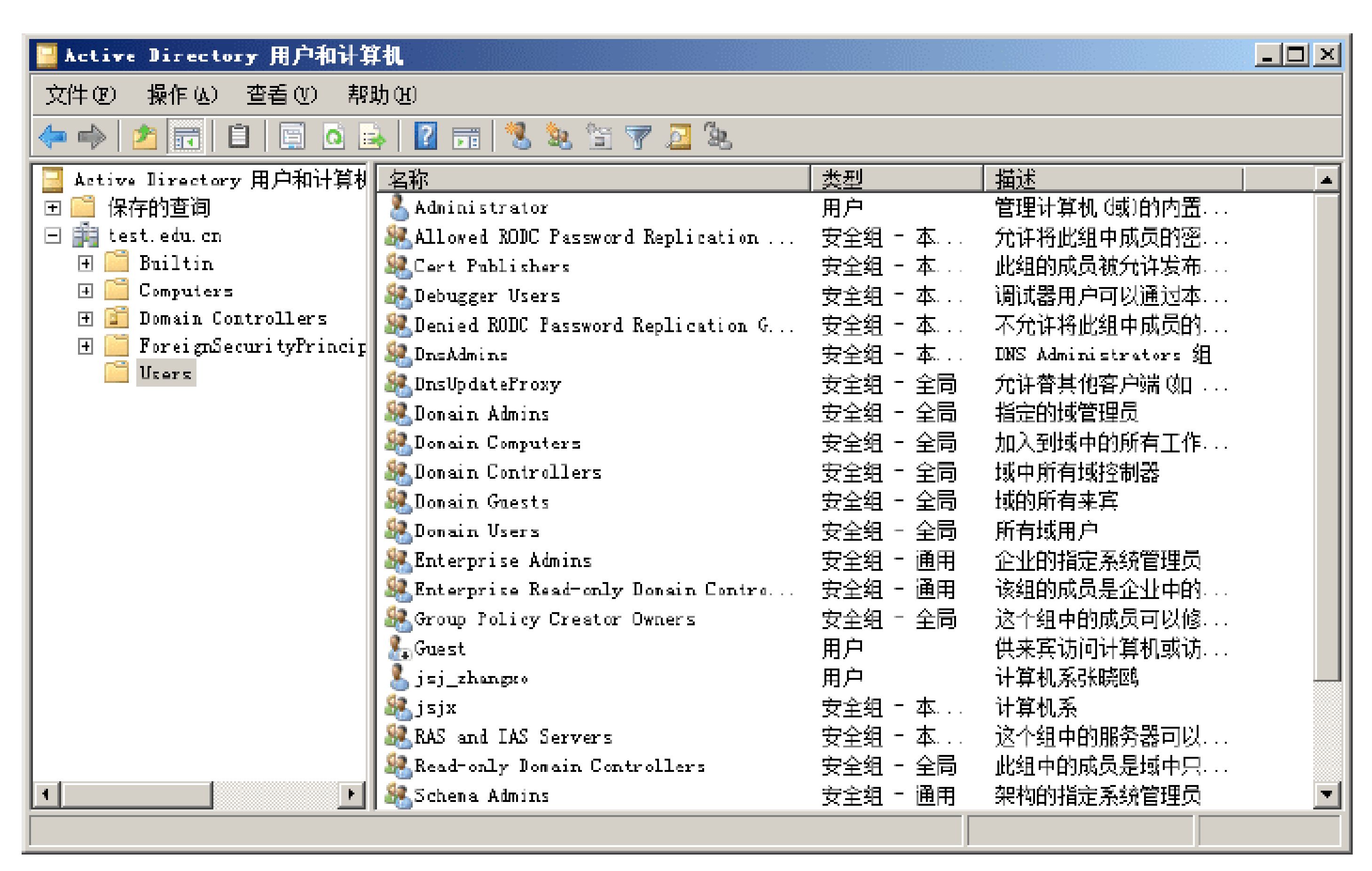


图 5-49　“Active Directory 用户和计算机”窗口

在安装过程中 Windows Server 2008 活动目录(AD)中自动创建了 4 种内置的组，包括内置本地域组、内置全局组、内置通用组和特殊组。这些内置的组不能改名，也不允许删除。

(1) 内置本地域组

这些组本身已经被赋予了一些特殊的权利与权限，以便让这些组的成员具备管理活动目录的能力。只要将用户帐户或全局组等加入到这些内置本地域组中，那么这些用户帐户或全局组的帐户将从本地域组中继承相应的权利和权限。

注意：

这些内置的本地域组位于活动目录的 Builtin 组织单元内，本地域组行使权利的范围仅限于本域。

- Account Operators(用户帐户操作组)：为管理员组分配的许多权限都划分到这个组内。组的成员可以在“Active Directory 用户和计算机”内创建、更改、删除及管理域内的用户帐户与组、重新设定密码、修改登录时间、修改配置文件和登录脚本、解除对用户帐户的锁定、对用户进行重命名。

但 Account Operators 组的成员不能修改、删除 Administrators、Domain Admins、Server

Operators、Backup Operators 或 Printer Operators 这些 Operators 组的属性和组中的成员。

- Administrators(管理员组)：凡是属于此 Administrators 本地域组内的用户，具有系统管理员的权限，拥有对整个域控制器最大的控制权，可以执行活动目录的管理任务，是活动目录中权力仅次于 Enterprise Adminis 的一个组，内置的系统管理员帐户 Administrator 就是该本地域组的成员，而且不能从该组中删除。因此，必须避免将普通用户加入到该组中。默认包含 Administrator、Domain Admins、Enterprise Admins 组。
- Backup Operators(备份操作员组)：此组的成员可以登录 DC(域控制器)，无论对要备份的文件夹或文件是否具有访问的权限，能利用 Windows Server Backup 程序来备份或还原域控制器内的文件或文件夹。
- Certificate Service DCOM Access：分布式组件访问证书颁发组。允许此组的成员连接到单位或部门中的证书颁发机构。
- Cryptographic Operators：组中的授权用户可执行加密操作。既可加密自己的文件，也可加密其他用户的文件。
- Distributed COM Users：此组中的成员允许启动、激活和使用此计算机上的分布式 COM 对象。
- Event Log Readers：组成员可从本地计算机读取事件日志。
- Guests(来宾组)：此组是供没有用户帐户而需要临时访问活动目录资源的临时用户使用。此组默认的成员为 Guest、Domain Guests 等。
- IIS_IUSRS：Internet 信息服务使用的内置组。此组的用户可上传文件，编辑网页。
- Incoming Forest Trust Builders(创建林信任关系组)：只有根域才会有此组，此组的成员可建立与另外一个林的单向或双向信任关系。
- Network Configuration Operators(网络配置组)：此组的成员可在域控制器上执行一般的网络设置工作，例如，更改 IP 地址等 TCP/IP 设置等，但是不能安装或删除网络硬件的驱动程序与服务，也不能执行除 TCP/IP 外与网络服务器设置有关的任务，例如，不能设置 DNS、DHCP 服务器。
- Performance Log Users(性能日志访问组)：此组的成员可以从远程计算机上访问、设置此计算机上的性能计数器的日志(查看“性能”中的性能日志和警报)，以便从远程计算机上了解服务器状况。
- Performance Monitor Users(性能监控组)：此组的成员可以远程访问、监视此计算机的操作(查看“性能”中的系统监视器)，以便从远程计算机上了解或设置性能计数器。
- Pre-Windows 2000 Compatible Access(与 Windows 2000 以前版本兼容的访问组)：此组的成员是 Windows 2000 以前版本操作系统的用户或组，允许此组的成员访问 Windows 2000/2003/2008 活动目录中的资源，设置该组主要从兼容性考虑。
- Printer Operators(打印组)：此组的成员可完全控制活动目录中的共享打印机。该组对打印机具有完全控制的权限，即可设置打印机的属性、决定是否共享打印机，而

普通用户默认只允许使用打印机。

- Remote Desktop Users(远程桌面组)：该组的成员可以远程登录、访问桌面系统，像本地登录用户那样使用和配置计算机。
- Replicator(复制组)：此组的成员专门用来执行复制目录服务时使用(一般不需要向该组添加实际用户)。单独一个域时此组为空，多域时则默认登录域控制器的用户就是该组的成员。
- Server Operators(服务器维护组)：拥有登录域控制器、系统关机、备份、还原、更改系统时钟、从远程强制关机、管理磁盘、打印机、锁定与解锁域控制器、设置共享文件夹等功能；但不能改变系统安全性设置，不能创建帐户和组，不能设置TCP/IP，不能修改主机名等，主要负责域控制器的管理操作。
- Terminal Server License Servers(终端服务授权组)：终端服务许可证服务器，该组的用户允许设置终端服务以及相关的授权操作。
- Users：默认的普通的域帐户都是此组的成员。此组的默认成员为 Domain Users 全局组，在默认下，创建的普通用户自动加入该组。
- Windows Authorization Access Group：该组的成员可以访问 User 对象上的计算机的 tokenGroupsGlobalAndUniversal 属性。
- Allowed RODC Password Replication Group：允许组的成员将此组成员的密码复制到域中所有的只读域控制器中。
- Cert Publishers：Windows Server 2008 专门为活动目录提供认证服务和办理代理服务的组。其成员可设置数据恢复代理、颁发证书等代理服务。主要针对系统的一些服务，如 DHCP、DNS、Web、E-Mail 的访问许可证书的颁发。
- Denied RODC Password Replication Group：不允许此组的成员将此组成员的密码复制到域中所有的只读域控制器中。
- DHCP Administrator：DHCP 管理员组，此组的成员可设置 DHCP 服务器。
- DHCP user：所有自动获取 IP 地址的用户都是此组的成员。当安装了 DHCP 服务器后，就有它和下面的 DHCP Administrator 组。
- DnsAdmins：DNS 管理员组，可设置 DNS 服务器。
- RAS and IAS Servers：这个组中的服务器是为远程访问服务或 Internet 接入服务提供远程访问或接入服务的计算机，域中所有远程访问服务器都是该组的成员，可添加或删除。RAS 为远程访问服务的缩写，IAS 为 Internet 接入服务的缩写。

(2) 内置全局组

这些组本身没有任何权利与权限，但是可以通过将其加入到具备权利或权限的本地域组，或者直接给这些全局组或通用组指派权利或权限。这些内置的全局组位于 Users 容器内，常用的有：

- DnsUpdateProxy：此组的成员具有在 DHCP 服务器上代替 DHCP 客户端更新 DNS 资源记录的权限。将经过授权的 DHCP 服务器加入到该组，则当某 DHCP 服务器发生故障时，可由该组的其他 DHCP 服务器更新。该组仅存在于活动目录中，可

向该组添加 DHCP 计算机帐户，添加用户帐户则没有意义。

- Domain Admins：域管理员组，此组自动加入 Administrators 本地域组内，因此 Domain Admins 这个全局组内的每个成员也都具备域管理员的权限，此组默认的成员为 Administrator。

如果要使某个用户具有某域管理员权限来协助系统管理员管理该域，最好将这个用户加入 Domain Admins 全局组，而不要加入 Administrators 本地域组内，因为根据全局组的性质，Domain Admins 全局组不仅可以被加入到本域的其他本地域组，还可以加入到其他域内的本地域组和通用组，而 Administrators 组只能够被加入到同一个域内的其他本地域组内。可通过查看组属性的“成员”和“隶属于”来印证。

- Domain Computers：域计算机组。所有加入域的计算机帐户都是这个组的成员。
- Domain Controllers：域控制器组。域中所有的域控制器都是这个组的成员(主域控制器和额外域控制器，不包括父域及子域)。
- Domain Guests：域来宾全局组。Domain Guests 自动加入 Guests 本地域组内。而 Domain Guests 默认的成员为 Guest，开启 Guest，任意用户都可以持 Guest 来宾帐号访问域。
- Domain Users：域用户组。此组自动加入 Users 本地域组内。此组默认的成员为 Administrator，而以后所有添加的域用户帐户都自动属于此 Domain Users 全局组。
- Group Policy Creator Owners：此组的成员可修改域或组织单元的组策略，但不能创建和删除域或组织单元的策略。
- Read-only Domain Controllers：此组的成员是域中只读域控制器。

(3) 内置通用组

- Enterprise Admins：企业管理员组，如果希望某个用户具备管理整个活动目录的权利，则可以将此用户的帐户加入到 Enterprise Admins 通用组中，系统自动把此组加入到每个域的 Administrators 本地域组内，所以 Enterprise Admins 组的成员就可以管理活动目录中的所有域。此组默认的成员为 Administrator，企业管理员组只存在于根域(整个活动目录中仅有一个)，根域的系统管理员是这个组的成员(也是各域的域管理员组 Domain Admins 的成员)，其组内的成员可登录任何域控制器，而其他域的系统管理员是不能登录活动目录中其他域控制器的。
- Enterprise Admins Only-read Domain Controllers：该组的成员是根域的只读域控制器。
- Schema Admins：架构管理员组，本组的成员可改变域林的结构，包括改变全局编录的存储对象及属性。在默认情况下，该组唯一的成员是根域域控制器上的系统管理员。

(4) 特殊组

在“计算机管理”或“Active Directory 用户和计算机”的 Builtin 和 User 之外，还有多个中没有出现的系统组，这些组只有在给资源分配权限、设置权利时才能在 ACL(访问控制列表)中看到，组中成员是隐含的，表示可访问资源的一类用户。这些系统组与权限的关系，在第 2.2 节的“NTFS 权限”中已有介绍。

- Everyone：每人组。凡是访问域(针对活动目录)或本地计算机(独立服务器、成员服务器、工作站)的所有用户，都属于这个组。包括合法域用户、通过“网上邻居”或“网络”访问的用户、Guests 组等。例如，默认情况下，硬盘、所有文件夹和文件是允许 Everyone 访问的。Windows Server 2003/2008 中匿名用户 anonymous 不属于该组(Windows 2000 Server 属于该组)。

在 Windows Server 2003/2008 中，Everyone 组包括 Authenticated、Users + Guest。在更早期的操作系统版本中，Everyone 组包括 Authenticated、Users、Guest、Anonymous Logon。

- authenticated Users：所有经过域控制器身份验证、不管是本地登录还是网络登录的合法用户，都属于此组。有时，为了安全起见，在设置资源的访问权限时，使用 Authenticated Users 组而不要用 Everyone 组。
- interactive：交互组。任何在本地登录的用户(不是从“网上邻居”登录)，都属于这个组。与之对应的是 network。
- network：网络登录组。任何通过网络连接计算机的用户(即通过“网上邻居”、“远程登录”、“远程桌面”、“远程协助”登录)，都属于这个组。这个组与 interactive 组对应。
- creator Owner：创建所有者组。包括创建对象或取得对象所有权的用户帐户，例如，文件夹、文件或打印文件等资源的建立者，就是此资源的 Creator Owner(建立者/所有者组)。
- Anonymous Logon：匿名登录组。不需经过 Windows Server 2008 身份认证即可登录的用户，都属于这个组。例如，不必输入用户名和密码就可浏览 Web 站点的用户和下载文件的匿名 FTP 用户。
- Dialup：拨号连接组。任何利用拨号方式连接域的用户，都属于这个组。

内置系统组还有很多，一般不常用。

2. 域用户帐户和组的创建及属性设置

(1) 为域用户创建帐户

在域的用户管理中，对帐户具有添加、修改、删除等管理权限的用户或组如下：

- 系统管理员
- Administrators 组的成员
- Domain Admins 组
- Enterprise Admins 组
- Account Operators 组的成员

建立域帐户的步骤如下：

① 选择桌面左下角的“开始”→“管理工具”→“Active Directory 用户和计算机”命令，打开如图 5-50 所示的窗口，单击域名 test.edu.cn 左侧的“+”号，右击 Users 选项，在弹出的快捷菜单中依次选择“新建”→“用户”命令。



图 5-50　打开新建用户帐户

② 在如图 5-51 所示的对话框中，输入姓、名，用户登录名。



图 5-51　输入姓、名，用户登录名

③ 用户登录名即帐户名称，一般不超过 20 个字符，最好不用中文。帐户名与前面输入的“姓”、“名”或“姓名”可以相同，也可以不同，用于显示的帐户名称最好是实际的名称，便于查询。

④ 单击图 5-51 中的“下一步”按钮，打开如图 5-52 所示的界面，输入密码，根据需要选择帐户属性的 4 个复选框。默认输入的密码要求具有一定的复杂性，即大写字母、小写字母、数字以及其他字符，并且不能与帐户名一样，不能包含用户姓名，超过连续两个字符。



图 5-52　输入密码、选择帐户属性

⑤ 单击“下一步”按钮，然后单击“完成”按钮，完成域用户的创建，返回图 5-53

所示的窗口，右击帐户对应的用户姓名，可以对帐户进行删除、重命名、属性更改等管理操作。

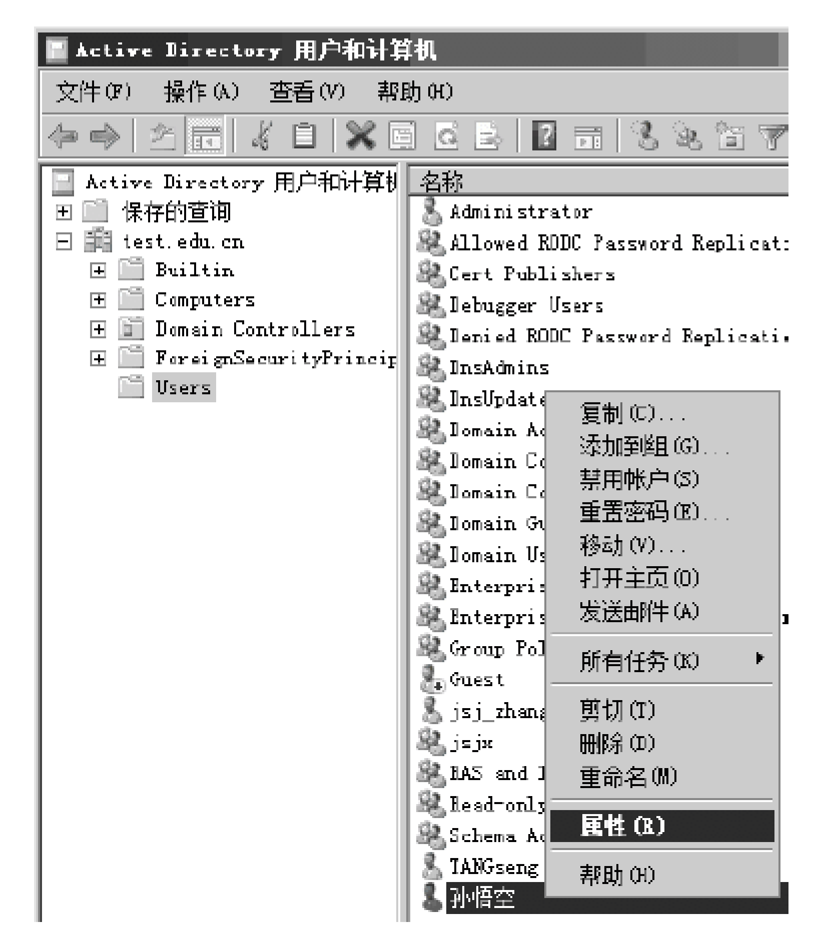


图 5-53　域帐户的管理

⑥ 若选择“属性”命令，在打开的如图 5-54 所示的对话框中，打开“帐户”选项卡，单击“登录时间”按钮，设置帐户登录域的时间。

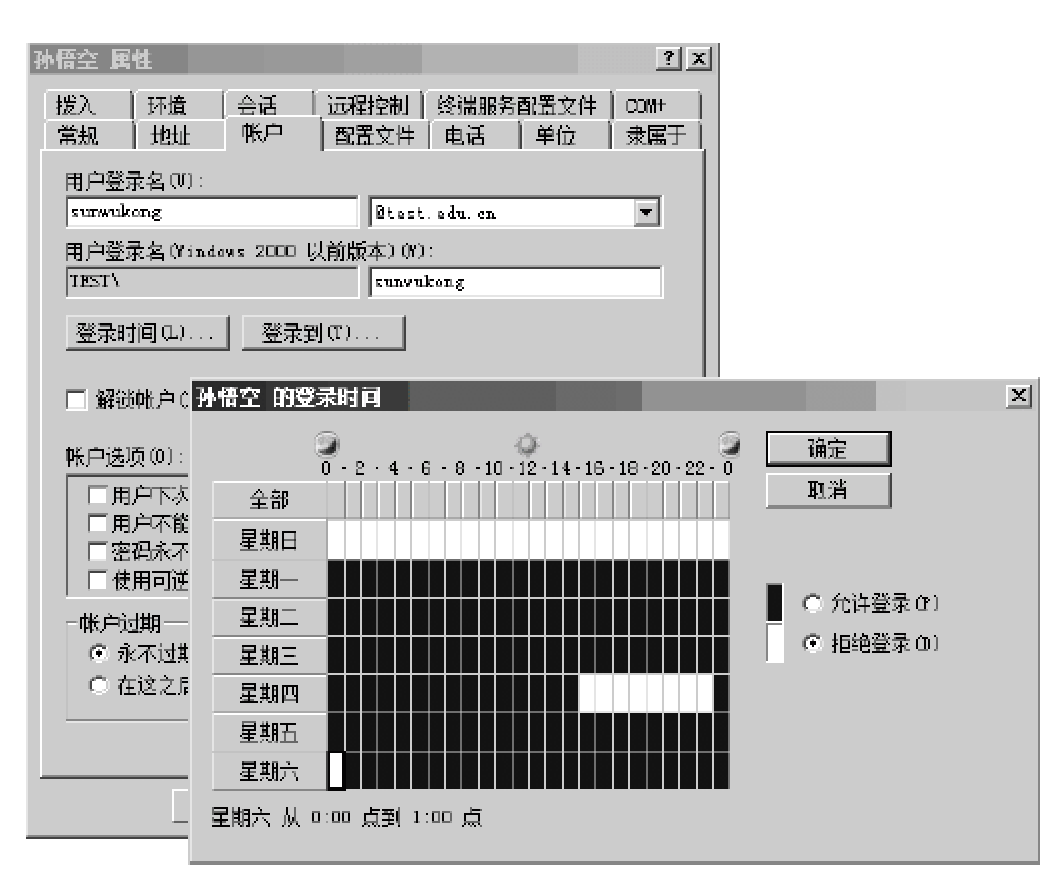


图 5-54　设置帐户登录域的时间

⑦ 所建立的域用户帐户，可以在成员服务器或工作站计算机上登录活动目录，但是却不能在域控制器登录，否则将出现提示：“系统不允许采用交互式登录”，除非帐户被授予“本地登录”的特权(在域控制器安全策略中的“安全设置”→“本地策略”→“用户权限分配”中指派)或被加入具有登录域控制器权限的组中，像 Administrators、Server Operators、Account Operators、Enterprise Admins、Domain Admins 组，系统管理员不要轻易让普通用户登录域控制器。

(2) 为域用户的帐户创建组

建立域帐户组的步骤如下：

① 在如图 5-55 所示的窗口中，右击 Users 选项，依次选择“新建”→“组”命令，打开如图 5-56 所示的对话框，输入组名，选择组的作用域和类型。

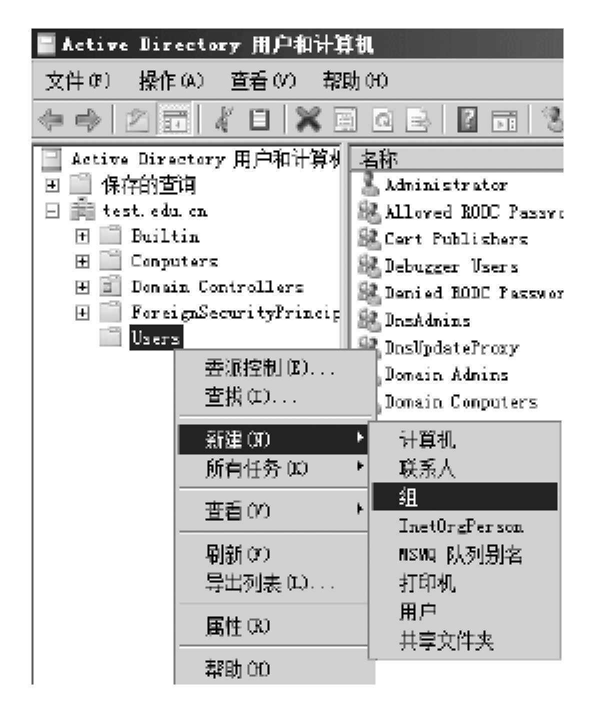


图 5-55　新建域用户帐户组



图 5-56　输入组信息、选择组的作用域和类型

② 单击“确定”按钮，完成组的创建，返回图 5-57 所示的窗口。右击组名，利用弹出的快捷菜单，可对该组进行删除、重命名、修改组属性等管理工作。



图 5-57　管理组

③ 在如图 5-57 所示的快捷菜单中选择“属性”命令，将打开的对话框切换至“成员”选项卡，单击“添加”按钮，接着单击“高级”按钮，如图 5-58 所示。



图 5-58　添加组的成员帐户

④ 单击“立即查找”按钮，拖动垂直滚动条浏览帐户，选择欲添加的成员帐户，如图 5-59 所示，单击“确定”按钮。



图 5-59 浏览选择欲添加的成员帐户

⑤ 返回如图 5-60 所示的界面，单击“确定”按钮，完成成员帐户的添加。



图 5-60 添加组的成员帐户

按照以上操作过程，为该组添加其他帐户，建立其他所需的帐户、组，并将每个帐户加入所属的组中。

5.3.3 组织单位

1. 概述

在 Windows NT 时代，域(Domain)是组织和管理网络的最小单位。倘若单位不同的部门有不同的安全需求与管理方式，有些部门也许只有几个人，如人事部，若每个域至少要有一台域控制器，还要有域管理员，不仅增加了费用的支出和人力的占用，而且由于域之间要进行目录数据复制(域控制器到域控制器，域控制器到全局编录服务器)，加大了网络流量。因此往往需将整个单位划分成多个域，可是这种多域的架构，会增加管理负担。

为了解决这类问题，微软公司在域中增加了组织单位(或组织单元)这种对象，使得整个域的规划与管理更有弹性，能发挥“分层负责、授权管理”的优点。

2. 特点

- 不设组织单元的服务器和管理员，降低了目录管理的复杂性和成本。
- 可以对其进行委派和设置组策略，即组织单元是委派控制、设置组策略的最小应用单元。
- 默认组织单元不属于安全体系范畴，不能为组织单元设置安全选项或分配权限。
- 组织单元可包含多种对象，也可多层嵌套，其中的对象可在组织单元中随意迁移。

3. 创建组织单位

能包含其他对象的对象便称为容器(Container)。组织单位是一种容器，它可以包含以下 9 种对象：用户、计算机、组、打印机、共享文件夹、联络人、其他组织单位、InetOrgPerson、MSMQ 路由别名。可以基于地理位置、功能、组织或它们的结合，对组织单位进行划分(如图 5-61 所示)。

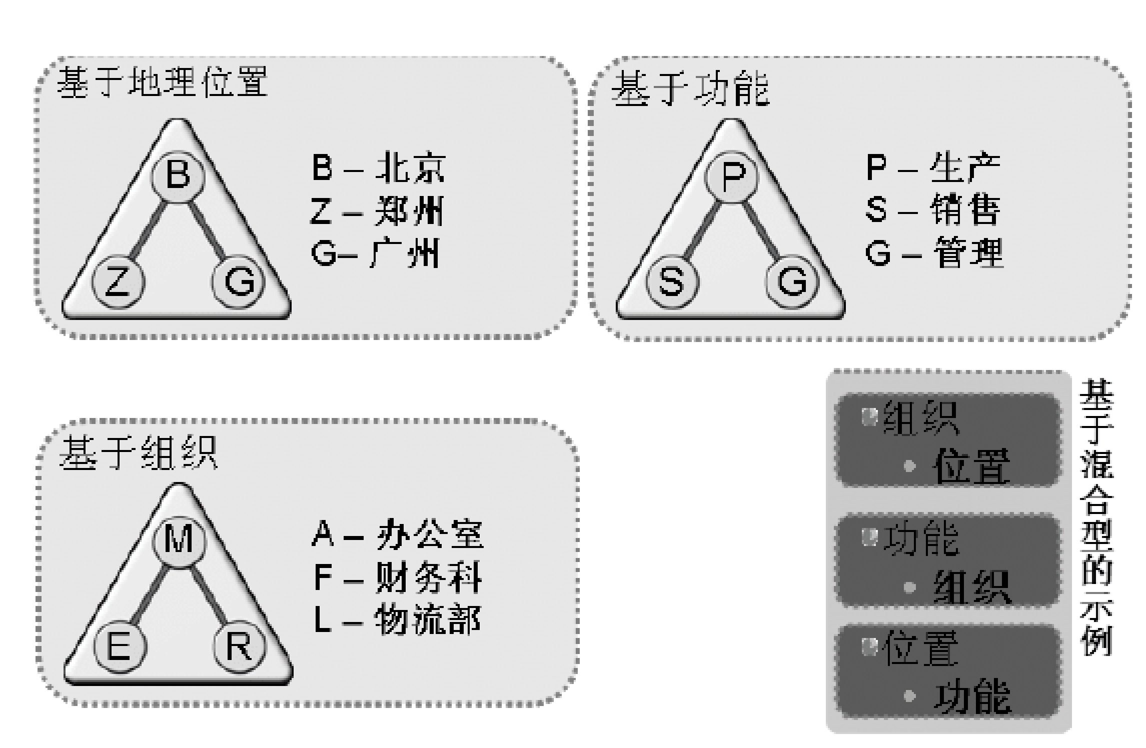


图 5-61　常见的组织单位规划模式

注意：
组织单位仅能包含同域内的对象，不能包含其他域的对象。

组织单位与组(Group)都应用在域的逻辑架构中，但在使用上有以下差异：

- 一个用户可以隶属于多个组，但是只能隶属于一个组织单位。
- 组织单位可以包含组，但是组不能包含组织单位。
- 网络资源(例如，文件夹或打印机)的权限可以赋予组，但是不能赋予组织单位。

组织单位的建立步骤如下：

(1) 单击桌面左下角的“开始”按钮，选择“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开相应的窗口，如图 5-62 所示，右击域名 test.edu.cn，从弹出的快捷菜单中选择“新建” →“组织单位”命令，弹出如图 5-63 所示的对话框。



图 5-62　新建组织单位



图 5-63　录入组织单位名称

(2) 输入组织单元的名称。组织单元名称可以包含中文，但最长为 64 个字符。单击“确定”按钮完成创建。

(3) 建立其他需要的组织单位，如图 5-64 所示。

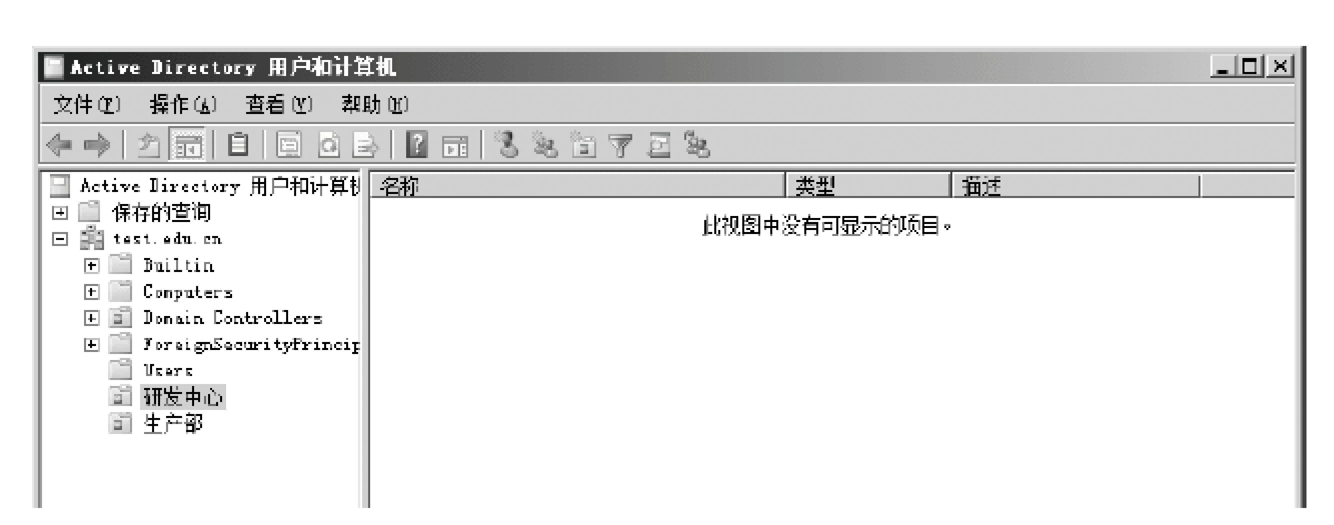


图 5-64　建立其他需要的组织单位

4. 建立、管理组织单位的成员

建立、管理组织单位的成员的步骤如下：

(1) 添加域用户帐户。如图 5-65 所示，右击某组织单位，从弹出的快捷菜单中选择“新建”→“用户”命令，按照建立帐户的过程创建组织单位的用户帐户。

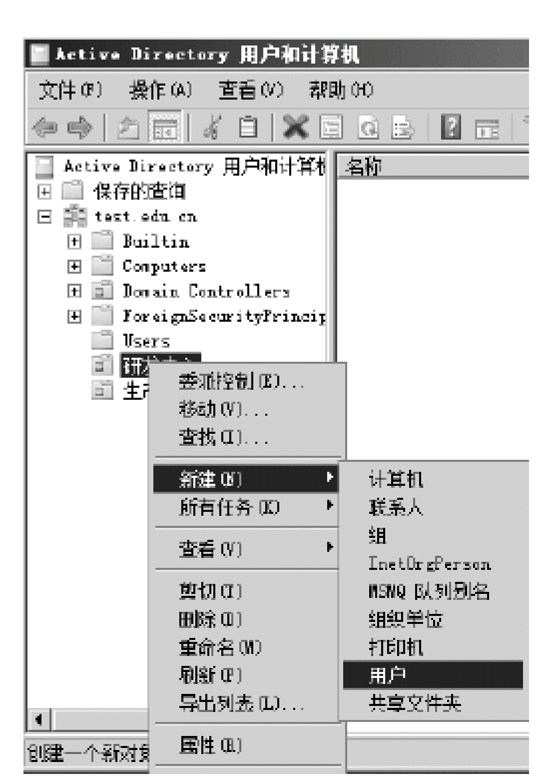


图 5-65　为组织单位新建用户帐户

(2) 添加域用户的帐户组。如图 5-66 所示，单击 Users 选项，右击域中某用户帐户组，从弹出的快捷菜单中选择“移动”命令，弹出如图 5-67 所示的对话框。



图 5-66　域用户的帐户组添加到组织单位



图 5-67　选择组织单位

(3) 选择某组织单位，单击“确定”按钮完成添加。

(4) 添加计算机帐户。在图 5-65 中选择“新建”→“计算机”命令，弹出如图 5-68 所示的对话框，输入计算机名称，单击“确定”按钮，完成向组织单位内添加计算机帐户。

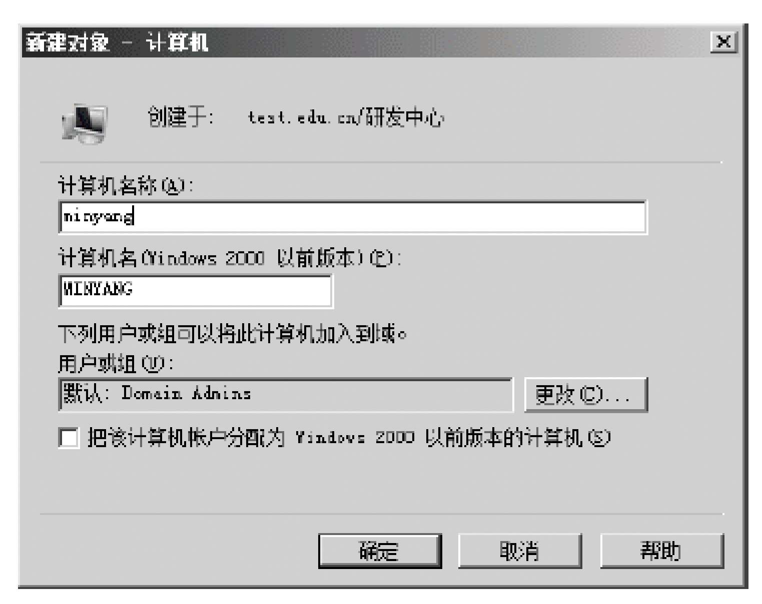


图 5-68　向组织单位内添加计算机帐户

(5) 右击某个组织单位，弹出快捷菜单，可以进行删除、重命名、属性更改等管理操作。

5.4　计算机加入、脱离域

安装有 Windows 的计算机加入域后可作为成员服务器或工作站。

独立服务器是指安装了 Windows Server 的计算机，独立服务器一旦加入域后，即可被配置成不同用途的专业服务器，按其提供的服务的不同，冠以不同的名字，例如：FTP 文件服务器、打印服务器、数据库服务器、Web 服务器、新闻服务器、多媒体服务器等，这些具有一定特殊功能的服务器称为成员服务器。

成员服务器仍保留本地帐户数据库，因此用户也可以利用这些本地帐户登录这些服务器，即登录时即可以选择是登录本地还是登录域。

在域中除了域控制器、成员服务器外，任何加入域的计算机都被称作工作站，或称域控制器的客户端，它们同时也可以是成员服务器的客户端，加入域本质上是在域控制器上创建计算机帐户。从域控制器的 Active Directory 用户和计算机的 Computers 容器中可看到所有加入本域的计算机帐户。当计算机加入域而成为工作站后，用户可在工作站上登录域，访问域的资源。工作站由域控制器负责用户身份验证。例如：域系统管理员可以限制谁何时从工作站登录到活动目录。工作站上保存本地帐户数据，用户也可以利用这些本地帐户登录工作站，访问本地资源。充当工作站的操作系统可以是 Windows 98/2000/XP/2003/Vista/2008/7。

注意：

加入域的计算机先要配置到域控制器的通信连接，并且配置的 DNS 服务器地址与域控制器需一致。

5.4.1　加入域

登录要加入域的成员计算机时，一定要用本地系统管理员的身份登录。计算机加入域的步骤如下：

(1) 以系统管理员身份如 administrator 帐户登录本地计算机，如图 5-69 所示，右击“我的电脑”，选择“属性”命令，打开“系统属性”对话框，切换到“计算机名”选项卡，单击“更改”按钮。



图 5-69　“系统属性”对话框

(2) 弹出如图 5-70 所示的对话框，选中“域”单选按钮，输入要加入的域名，如 test 或 test.edu.cn，单击“确定”按钮。



图 5-70　输入域名

(3) 系统找到 DNS 服务器后，根据服务资源记录，找到域控制器，域控制器要求输入具有管理员权限的帐户名及密码，如 Administrator，如图 5-71 所示。



图 5-71　输入域控制器的管理员帐户名及密码

(4) 当申请加入域得到验证认可后，显示“欢迎加入 test 域”或“欢迎加入 test.edu.cn 域”，如图 5-72 所示，重新启动计算机后生效，计算机的名称默认会出现在“Active Directory 用户和计算机”窗口的 Computres 容器中，这个容器专门存放加入域的计算机帐户。



图 5-72　欢迎加入域

域中的计算机虽然只有帐户，没有密码，但当系统管理员将某计算机加入域后，域控制器与计算机之间会自动建立一把相同的密钥，域中的计算机各自都有与域控制器共享的密钥。

5.4.2　登录域

当计算机加入域后，用户启动计算机登录域时，可选择从本地登录，也可以登录到域，在多域环境下，可以访问任何域的资源。首先选择“登录到”后面的本机或域，然后输入本机的用户名、密码，或域管理员分配的域用户名、密码，登录到本地主机或域。

查看、使用域资源的一个方法是：选择“网上邻居”→“整个网络”→Microsoft Windows Network→欲访问的计算机、资源名称，即可在授权范围内访问域中资源。在成员计算机上，各个域的域用户都可以通过活动目录中某个工作站登录到域中。

没有加入域的计算机(域外计算机)即以工作组方式运行，这些计算机的帐户安全性设置都由本地自行管理。如果要通过“网上邻居”或“网络”访问域中的计算机，双击某一计算机图标时，出现登录对话框，输入域帐户登录名和密码，才可访问共享文件夹。而加入域的用户则不需输入登录名称和密码。

加入域的计算机与域外计算机访问活动目录资源，对于单个域优势并不明显，但对于多域环境来说，一次登录就可访问活动目录中所有域中有权访问的资源。一次登录也叫单点登录，或交互登录，区别于二次登录，从网络访问共享资源属于二次登录。而从工作站登录活动目录属于交互登录。

5.4.3　脱离域

用户可以脱离本域、加入其他域，但是需要通过域管理员的同意。操作方法如下：

计算机用户以管理员身份进行本地登录，右击“我的电脑”，依次选择“属性”→“计算机”→“更改”→“工作组”，输入工作组名后，单击“确定”按钮，输入域管理员的用户帐户名和密码，如图 5-73 所示，单击“确定”按钮，重新启动计算机。



图 5-73　输入域管理员的用户帐户名和密码

注意：

只有 Enterprise Users 或 Domain Users 组成员或本地系统管理员才有权将计算机脱离域。

5.5　组策略及应用

组策略与组织单位中的组不同。系统管理员可利用组策略来管理活动目录数据库中的计算机与用户。例如：用户桌面环境、计算机启动/关机的过程中所执行脚本文件，用户登录/注销过程中所执行的脚本文件、文件重定向、软件安装等。

5.5.1　组策略概述

组策略的设置数据保存在活动目录数据库中，因此必须在域控制器上设置组策略。组策略只能够管理计算机与用户，也就是说组策略是无法管理打印机、共享文件夹等其他对象的。组策略不能应用到组，只能够应用到站点、域或组织单位。组策略不适用于 Windows9X/NT 计算机，所以应用到这些计算机上无效。组策略不会影响未加入域的计算机和用户，对于这些计算机和用户，应使用本地安全策略来管理。

注意：

本地安全策略与组策略很相似，但功能较少，仅能管理本机上的计算机设置与用户设置。

组策略的设置数据都保存在“组策略对象(GPO)”中，GPO 具有以下特性：

(1) GPO 利用 ACL 记录权限设置，可以修改个别 GPO 的 ACL，指定哪些人对该 GPO 拥有何种权限。

(2) 用户只要有足够的权限，便能够添加或删除 GPO，但无法复制 GPO。当活动目录域刚建好时，默认仅有一个 GPO(默认域策略)。这个 GPO 可用来管理域中所有的计算机与用户。若要设置应用于组织单位的组策略，通常会再另行建立 GPO，以方便管理。

GPO 的策略有以下两种：

(1) 计算机配置。包含所有与计算机有关的策略设置，这些策略只会应用到计算机帐户。

(2) 用户配置。包含所有与用户有关的策略设置，这些策略只会应用到用户帐户。

如图 5-74 所示，单击桌面左下角的“开始”按钮，选择“管理工具”→“组策略管理”命令。



图 5-74　打开“组策略管理”

右击“Default-Domain-Policy”，如图 5-75 所示，在弹出的快捷菜单中选择“编辑”命令，打开如图 5-76 所示的窗口。



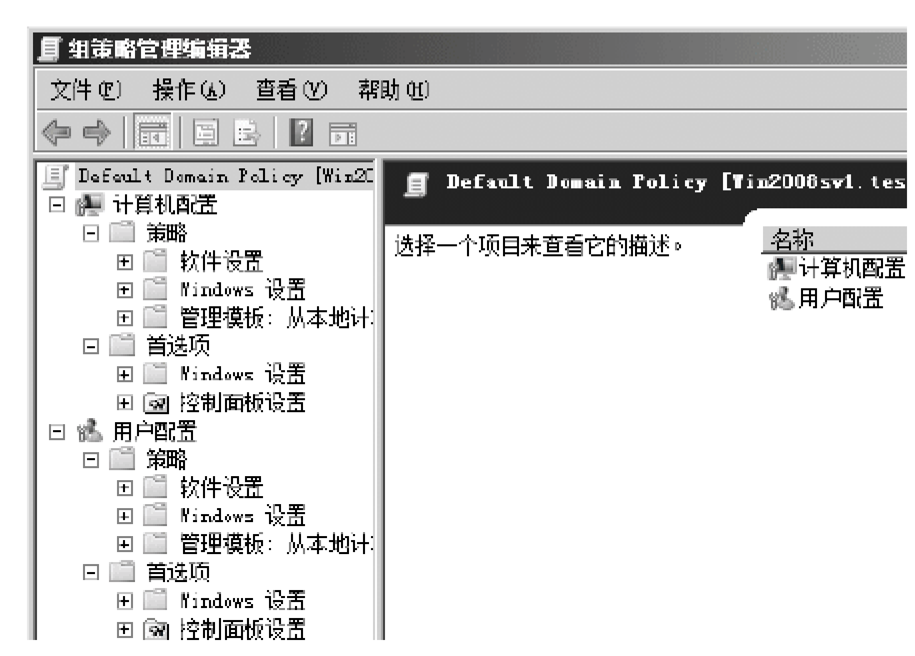


图 5-75　编辑 Default-Domain-Policy　　　图 5-76　Default-Domain-Policy 编辑窗口

在这个域树结构中，计算机配置和用户配置称为节点(node)。这两个节点又都包含了软件设置、Windows设置和管理模块 3 个子节点。

- 软件设置：此策略用来管理域内所有软件的安装、发布、指派、更新、修复和删除。
- Windows 设置：系统管理员能够设置脚本文件、建立帐户策略、指派用户权限和集中管理用户配置文件。Windows 设置在计算机设置与用户设置内，分别有不同的设置项目。在计算机设置的 Windows 设置中，能够设置脚本文件与安全性设置策略；在用户设置的 Windows 设置中，能够设置Internet Explorer维护、脚本文件、安全性设置、远程安装服务与文件重定向策略。

● 管理模板：与注册表有关的策略在该子节点下。系统管理模板在计算机设置能够设置 Windows 元件、系统、网络与打印机策略。在用户设置的系统管理模板，能够设置 Windows 元件、开始菜单、和任务栏、桌面控制台、网络与系统策略。

在活动目录结构中，若 A 容器下层还有 B 容器，则 B 容器便是所谓的子容器，A、B 容器两者间便存在策略继承关系。在默认情况下子容器会继承来自上层父容器的 GPO。

在整个继承关系中，最上层为站点，其下层为域与组织单位。若有多层组织单位，则下层组织单位会继承上层组织单位的 GPO。

策略累加机制和组策略的应用顺序有密切的关系，组织单位除了本身的组策略外，还会继承来自上层容器策略。子容器会首先应用继承来自上层容器的组策略，然后再应用本身的组策略，当上层的设置项目与下层的设置项目不同时，组策略的效果可以相加，但若是对同一个项目做不同的设置，则先应用的策略会被后来应用的策略覆盖。

当计算机开机时，域控制器会根据计算机帐户在活动目录中的位置，决定该计算机必须应用哪些 GPO，此时仅应用这些 GPO 中计算机设置的部分；用户登录时，即按 Ctrl+Alt+Delete 后，输入帐号和密码，域控制器会根据用户帐户在活动目录中的位置，决定该用户必须应用哪些 GPO，此时仅应用这些 GPO 中用户设置的部分。

一般而言，都是计算机顺利启动之后，用户才能用该计算机登录域，因此，在实际上是先应用计算机设置，后应用用户设置。当计算机设置和用户设置发生冲突时，计算机设置覆盖掉用户设置。

由于计算机与用户可能分别隶属不同的站点、域或组织单位，因此，各自可能会继承不同的 GPO。最先应用本机的组策略，其次为站点的组策略，然后为域的组策略，最后是组织单位的组策略。倘若不考虑不可强制覆盖和不要继承策略，策略则是“后应用的设置值覆盖先应用的设置值”。

5.5.2　创建组策略

创建组策略的操作步骤如下：

(1) 如图 5-77 所示，右击某组织单位或域名后，从弹出的快捷菜单中选择第一个命令，弹出如图 5-78 所示的对话框。

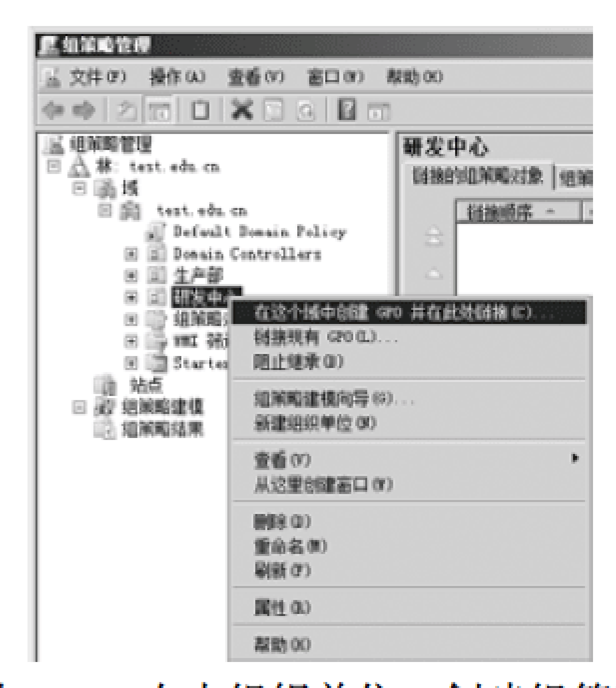


图 5-77　右击组织单位、创建组策略

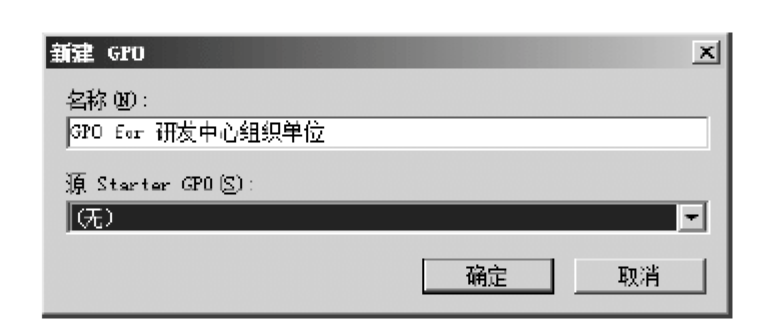


图 5-78　输入组策略名称

(2) 输入组策略名称，单击“确定”按钮。

(3) 单击组策略所属的组织单位左侧的“+”符号，如图 5-79 所示，单击组策略名称，单击右侧窗口中的“添加”按钮，设置组策略的约束对象，如图 5-80 所示。



图 5-79　单击“添加”按钮

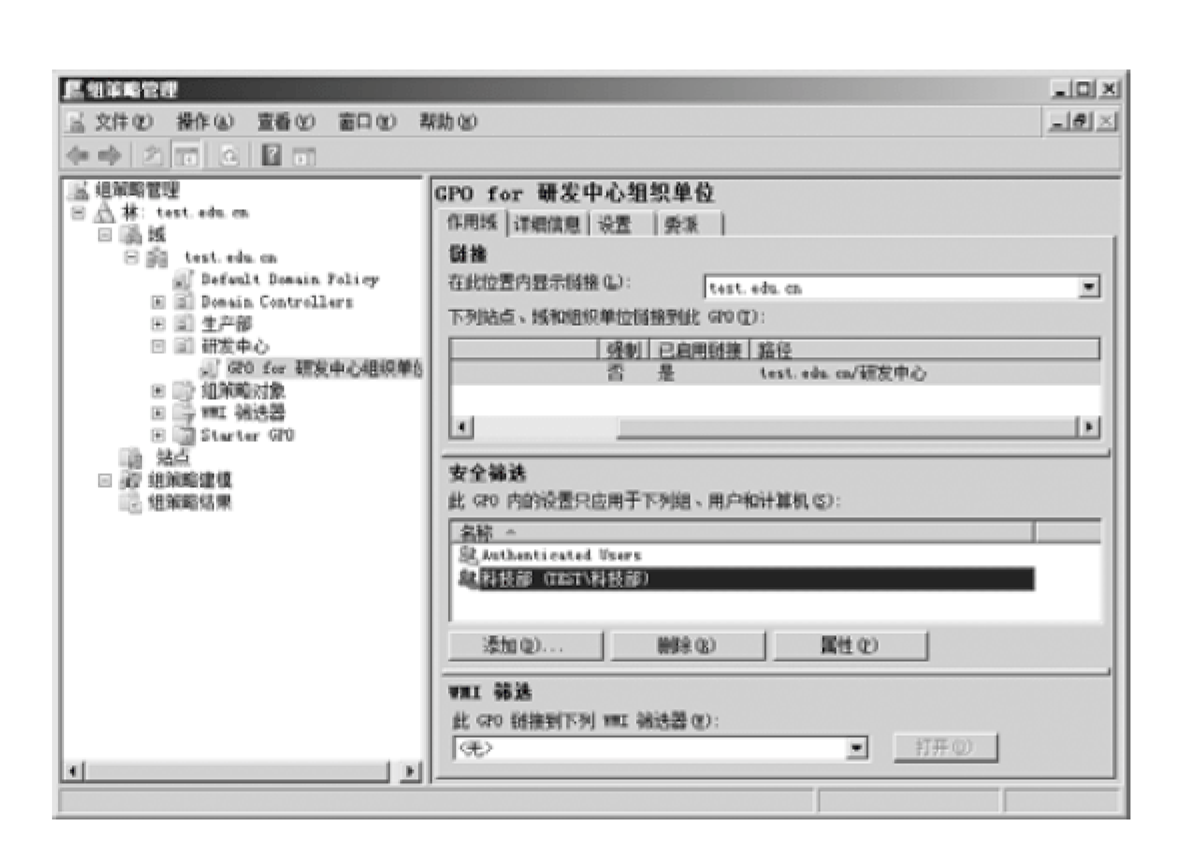


图 5-80　设置组策略的约束对象

(4) 切换到“委派”选项卡，如图 5-81 所示，将管理 GPO 的工作委派给特定的用户，单击“添加”按钮，浏览、添加用户的帐户或组，并设置管理组策略的权限，如图 5-82 所示，单击“确定”按钮。




图 5-81　“委派”选项卡



图 5-82　设置管理组策略的权限

(5) 打开帐户如(jsj_zhangxo)的属性对话框，单击打开“隶属于”选项卡，如图 5-83 所示，单击“添加”按钮，浏览、添加 GROUP POLICY CREATOR OWNER 组，使用户获得新建与删除 GPO 的权限。

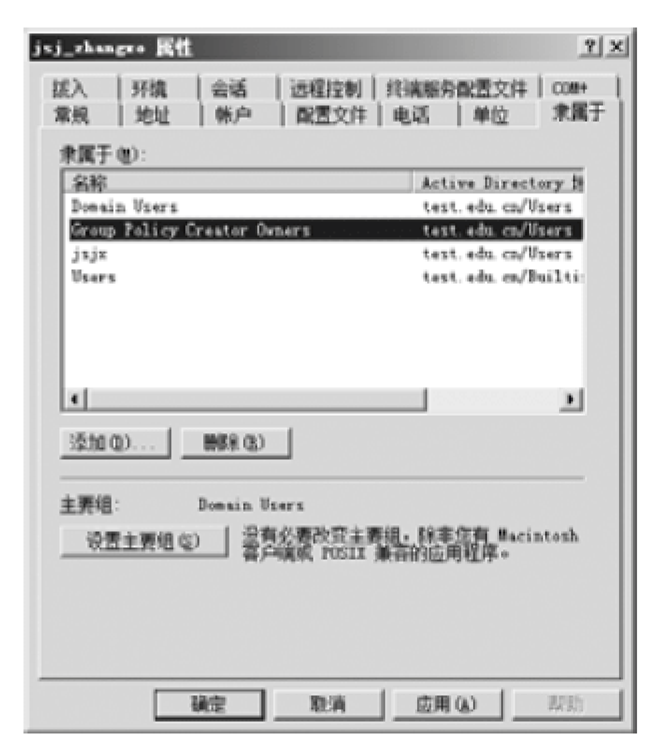


图 5-83　将帐户加入 GROUP POLICY CREATOR OWNER 组

(6) 如果希望强制被组策略约束的对象接受组策略的规则，可单击组策略所属的组织单位左侧的“+”符号，如图 5-84 所示，右击组策略名称，在弹出的快捷菜单中选择“强制”命令。

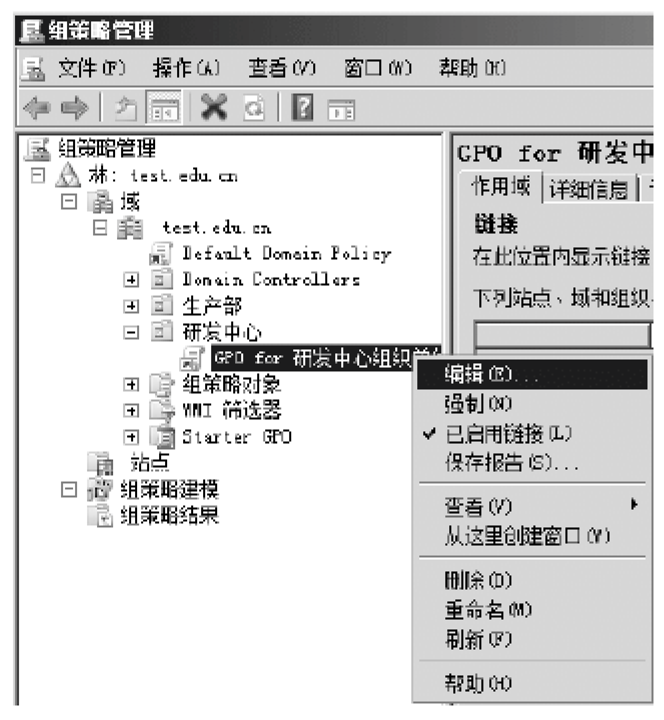


图 5-84　强制被组策略约束的对象接受组策略的规则

5.5.3　组策略的应用

巧妙地利用 Windows 系统自带的 ping 命令，可以快速判断网中某台重要计算机的网络连通性；可是，ping 命令在带来实用的同时，也容易被一些恶意用户所利用，例如恶意用户要是借助专业工具不停地向重要计算机发送 ping 命令测试包时，重要计算机系统由于无法对所有测试包进行应答，从而容易出现瘫痪现象。为了保证 Windows Server 2008 服务器系统的运行稳定性，可修改该系统的组策略参数，来禁止来自外网的非法 ping 攻击：首先以管理员身份登录进入 Windows Server 2008 服务器系统，选择“开始”→“运行”命令，输入命令 gpedit.msc，单击“确定”按钮，进入对应系统的控制台窗口，依次双击打开“计算机配置”节点下的“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙”→“本地组策略对象”命令，右击“入站规则”，如图 5-85 所示，在弹出的快捷菜单中选择“新规则”命令。

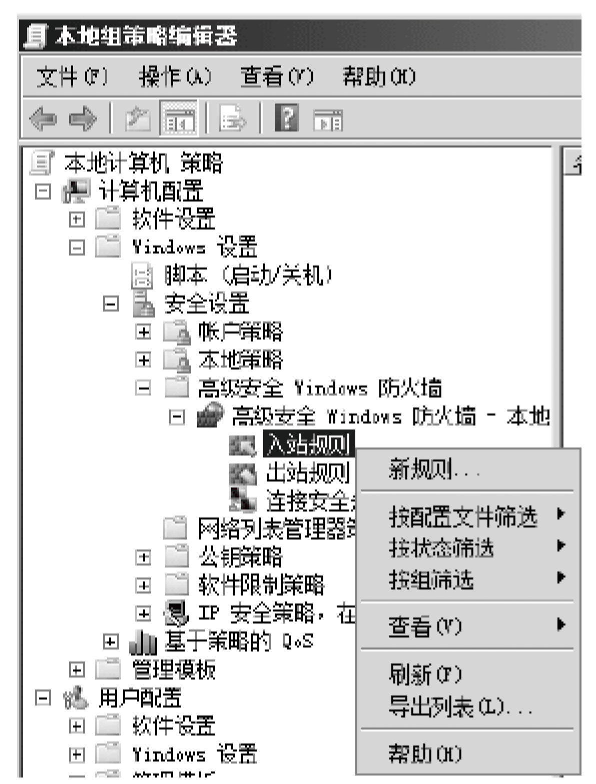


图 5-85　创建新规则

在“规则类型”中选择“自定义”→“程序”的“所有程序”，然后在“协议和端口”中选择协议类型 ICMPv4，如图 5-86 所示。



图 5-86　在协议类型列表中选择 ICMPv4

在“操作”界面中选择“阻止连接”，单击打开“名称”界面，如图 5-87 所示，输入规则的名称，单击“完成”按钮。

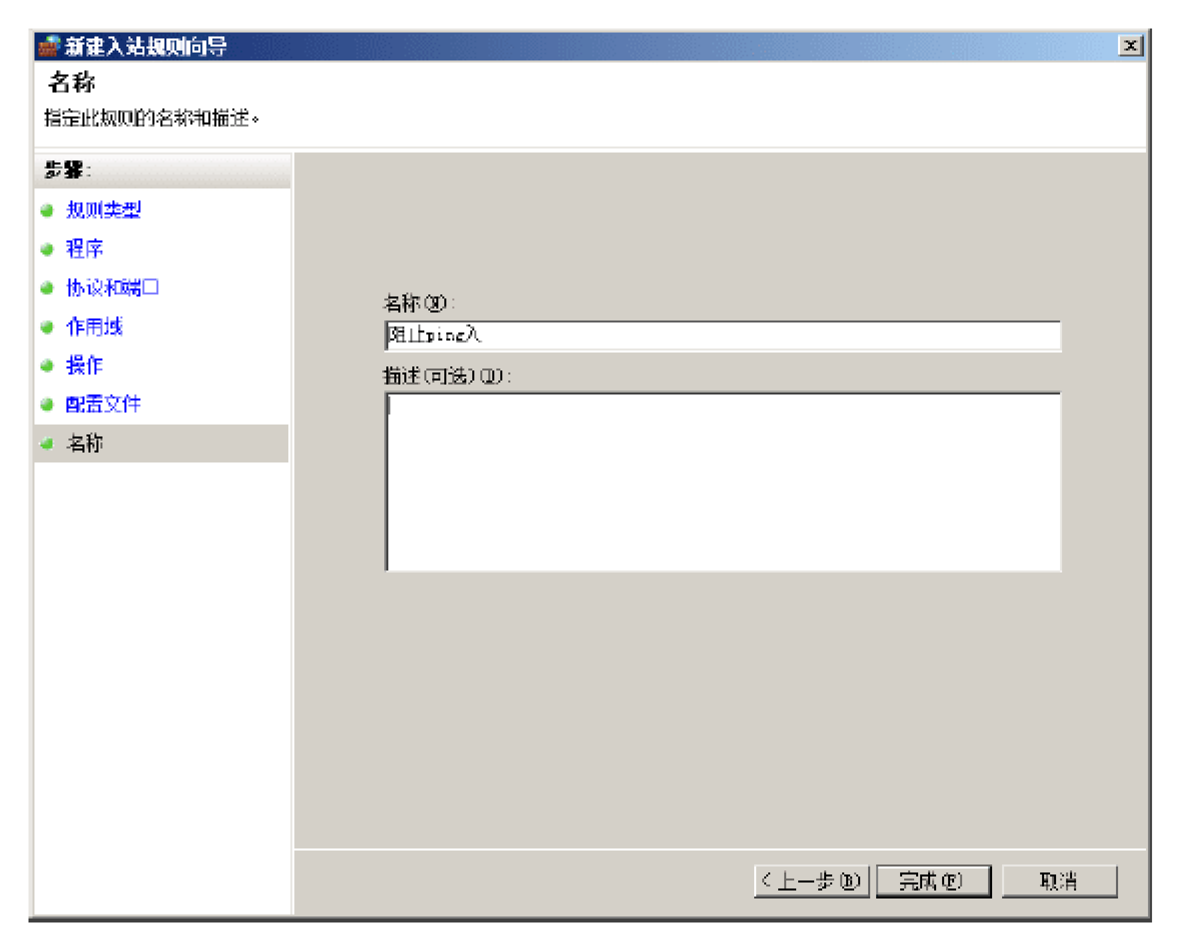


图 5-87　输入规则的名称

完成上面的设置后，重新启动计算机，Windows Server 2008 服务器系统能够阻止来自其他主机的非 ping 攻击。

5.6　本章小结

本章首先介绍 Windows Server 2008 的基于工作组网络的小规模应用，然后主要介绍了 Windows Server 2008 的活动目录功能。基于活动目录可构建大型的网络应用，同时提高网络的安全性和可管理性，主要内容包括：活动目录服务的功能、结构；活动目录的安装、配置与删除；用户与组的管理；Windows 计算机加入域、脱离域；组策略的创建及应用。

5.7　思考与练习

【思考题】

1. 活动目录的作用主要有哪些？其中对于信息安全的保障原理是什么？

2. 域用户组的作用是什么？分为几种？每种组的用途是什么？

3. 加入域后，Windows 客户端在没有登录域的状态下如何访问域中服务器与其他客户端的资源？

【练习题】

安装、配置、删除活动目录(参考 5.2 节)。

第6章　证书服务

【本章导读】

Windows Server 2008 提供了电子证书服务，用于通信双方的身份验证，从而建立起一种信任机制，在一定程度上保障了信息安全。本章主要介绍了电子证书服务与证书服务器的部署、企业 CA 的安装与使用、独立根 CA 的安装与使用、证书服务的管理。

6.1　电子证书服务

6.1.1　电子证书简介

为了保证网络上信息传输的安全，除了在通信中采用更强的加密算法等措施外，还必须建立一种信任及信任验证机制，即通信各方必须有一个可以被验证的标识，这就需要使用电子证书。证书的主体可以是用户、计算机、服务等。证书可以用于多方面，例如 Web 用户身份验证、Web 服务器身份验证、安全电子邮件等。安全证书确保网上传递信息的机密性、完整性、以及通信双方身份的真实性，从而保障网络应用的安全性。

6.1.2　证书服务器的部署

1. 公钥基础结构(PKI)

(1) 什么是 PKI

PKI(Public Key Infrastructure)是通过使用公钥技术和数字证书来确保信息安全，并负责验证数字证书持有者身份的一种技术。在 PKI 中，各参与方都信任同一个 CA(证书颁发机构)，由该 CA 来核对和验证各参与方的身份。

(2) PKI 的组成

PKI 由公钥加密技术、数字证书、CA(证书颁发机构)、RA(注册机构)等共同组成。数字证书用于用户的身份验证。CA 是一个可信任的实体，负责发布、更新和吊销证书。RA 接受用户的请求，负责将用户的有关申请信息存档备案，并储存在数据库中，等待审核，并将审核通过的证书请求发送给证书颁发机构。

(3) PKI 体系实现的功能

- 身份验证：确认用户的身份标识。

- 数据完整性：确保数据在传送过程中没有被修改。
- 数据机密性：防止非授权用户获取数据。
- 操作的不可否认性：确保用户不能冒充其他用户身份。

2. 公钥加密技术

(1) 公钥与私钥

公钥加密技术是 PKI 的基础，这种技术需要两种密钥：公钥和私钥。

公钥和私钥的关系如下：

- 公钥和私钥是成对生成的，这两个密钥互不相同，两个密钥可以互相加密和解密。
- 不能根据一个密钥来推算出另一个密钥。
- 公钥对外公开，私钥只有私钥的持有人才知道。
- 私钥应该由密钥的持有人妥善保管。

公钥与私钥配对使用，如果用公钥对数据加密，只有用相对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。

(2) 数据加密

数据加密确保只有预期的接收者才能解密和查看原始数据，从而保证了数据的机密性。传送数据时，发送方使用接收方的公钥加密数据，并将它传送。当接收方收到数据后，使用自己的私钥解密这些数据。

(3) 数字签名

数字签名的作用如下。

- 身份验证：接收方可确认该发送方的身份标识。
- 数据的完整性：证实消息在传递过程中内容没有被修改。
- 操作的不可否认性：其他用户不可能冒充该发送方发送消息。

用户可以通过数字签名确保数据的完整性和有效性，只需采用私钥对数据进行加密处理，由于私钥仅为用户个人拥有，从而能够证实签名消息的唯一性。

3. 使用 PKI 的协议

PKI 相关协议如下：

- SSL(Secure Socket Layer)，安全套接字层；
- HTTPS(Secure Hypertext Transfer Protocol)，安全超文本传输协议；
- IPSec(IP Security)；

负责发放证书的机构被称为 CA(Certificate Authority，证书颁发机构)，CA 是 PKI 公钥基础结构中的核心部分。CA 负责管理 PKI 结构下所有用户的数字证书，把用户的公钥与用户的其他信息捆绑在一起，在网上验证用户的身份。

PKI 系统中的数字证书简称为证书，它把公钥和拥有对应私钥的主体的标识信息捆绑在一起。数字证书由第三方机构 CA 签发。

证书包含以下信息：

- 使用者的公钥值。
- 使用者标识信息。
- 有效期。
- 颁发者标识信息。
- 颁发者的数字签名，用来证明使用者的公钥和使用者的标识信息之间的绑定关系是否有效。

CA 的核心功能就是颁发和管理数字证书，具体内容如下：

- 处理证书申请。
- 鉴定申请者是否有资格接收证书。
- 证书的发放，向申请者颁发、拒绝颁发数字证书。
- 证书的更新，接收、处理最终用户的数字证书更新请求。
- 接收最终用户数字证书的查询、撤销。
- 产生和发布证书吊销列表(CRL)。
- 数字证书的归档。
- 密钥归档。
- 历史数据归档。

证书的发放过程如下：

(1) 用户进行证书申请。

(2) RA(注册机构)确认用户。

(3) 证书策略处理。

(4) RA 提交用户申请信息到 CA。

(5) CA 用自己的私钥对用户的公钥和用户信息 ID 进行签名，生成电子证书。

(6) CA 将电子证书传送给批准该用户的 RA。

(7) RA 将电子证书传送给用户。

(8) 用户验证 CA 颁发的证书。

6.2　企业 CA 的安装与使用

6.2.1　安装企业 CA

具体步骤如下：

(1) 在域控制器上，单击桌面左下角的“开始”按钮，依次选择“管理工具”→“服务器管理器”→“角色”命令，打开“添加角色向导”，如图 6-1 所示，添加证书服务角色，单击“下一步”按钮。



图 6-1　打开“添加角色向导”

(2) 如图 6-2 所示，选择“证书颁发机构”和“证书颁发机构 Web 注册”，单击“下一步”按钮。

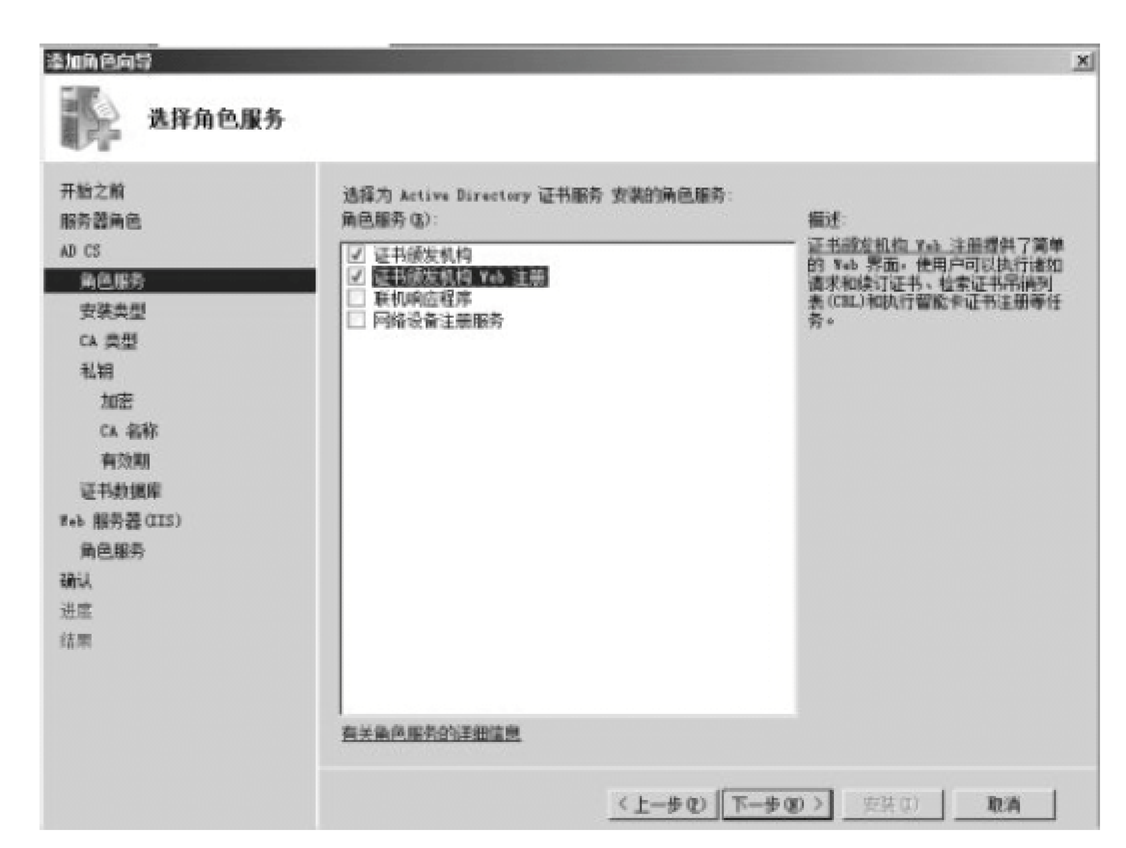


图 6-2　选择“证书颁发机构”和“证书颁发机构 Web 注册”

(3) 如图 6-3 所示，在指定安装类型中选择“企业”，单击“下一步”按钮。



图 6-3　指定安装类型

CA 分为两大类：企业 CA 和独立 CA。

企业 CA 的主要特征如下：

- 企业 CA 安装时需要 AD(活动目录服务支持)，即计算机在活动目录中才可以。
- 当安装企业根时，对于域中的所有计算机，它都将会自动添加到受信任的根证书颁发机构的证书存储区域。
- 必须是域管理员或对 AD 有写权限的管理员，才能安装企业根 CA。

独立 CA 主要有以下特征：

- 独立 CA 不需要 AD 服务。
- 向独立 CA 提交证书申请时，证书申请者必须在证书申请中明确提供所有关于自己的标识信息以及证书申请所需要的证书类型。
- 默认情况下，发送到独立 CA 的所有证书申请都被设置为挂起，一直到独立 CA 的管理员验证申请者的身份并批准申请。

这完全出于安全性的考虑，因为证书申请者的凭证还没有被独立 CA 验证。在简单介绍完 CA 的分类后，下面在 AD(活动目录)环境下安装证书服务。

(4) 如图 6-4 所示，选择“根 CA”，单击“下一步”按钮。



图 6-4　指定 CA 类型

企业 CA 和独立 CA 中又可以分为根 CA 和子级 CA：

- 根 CA 是指在组织的 PKI 中最受信任的 CA；
- 子级 CA 是由组织中的根 CA 颁发证书的 CA。

(5) 如图 6-5 所示，在“设置私钥”界面中选择“新建私钥”，单击“下一步”按钮。



图 6-5　设置私钥

(6) 如图 6-6 所示，在“为 CA 配置加密”界面，使用默认的加密服务程序、哈希算法和密钥长度，单击“下一步”按钮。

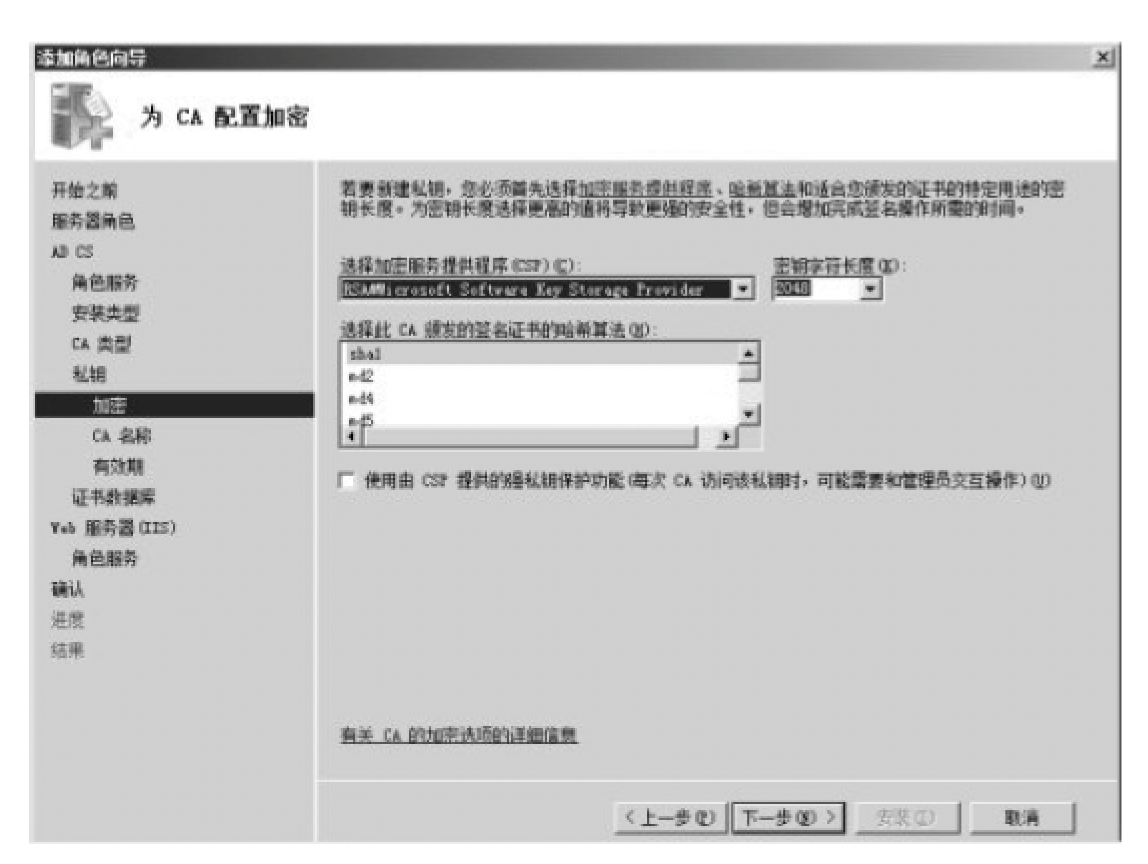


图 6-6　为 CA 配置加密

(7) 如图 6-7 所示，配置 CA 名称，单击“下一步”按钮。



图 6-7　配置 CA 名称

(8) 如图 6-8 所示，设置 CA 证书的有效期，默认为 5 年，单击“下一步”按钮。



图 6-8　设置 CA 证书的有效期

(9) 如图 6-9 所示，选择证书数据库的保存位置，单击“下一步”按钮。

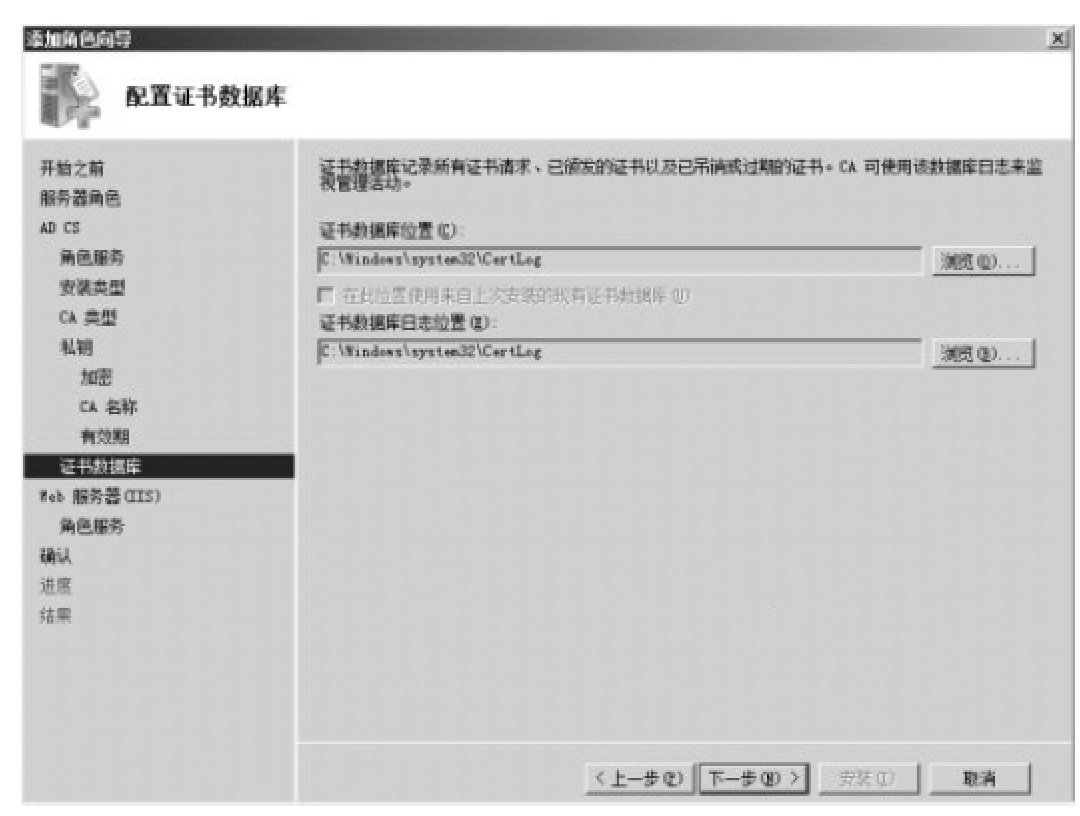


图 6-9　选择证书数据库的保存位置

(10) 如图 6-10 所示，安装 Web 服务器所必需的角色服务，单击“下一步”按钮。

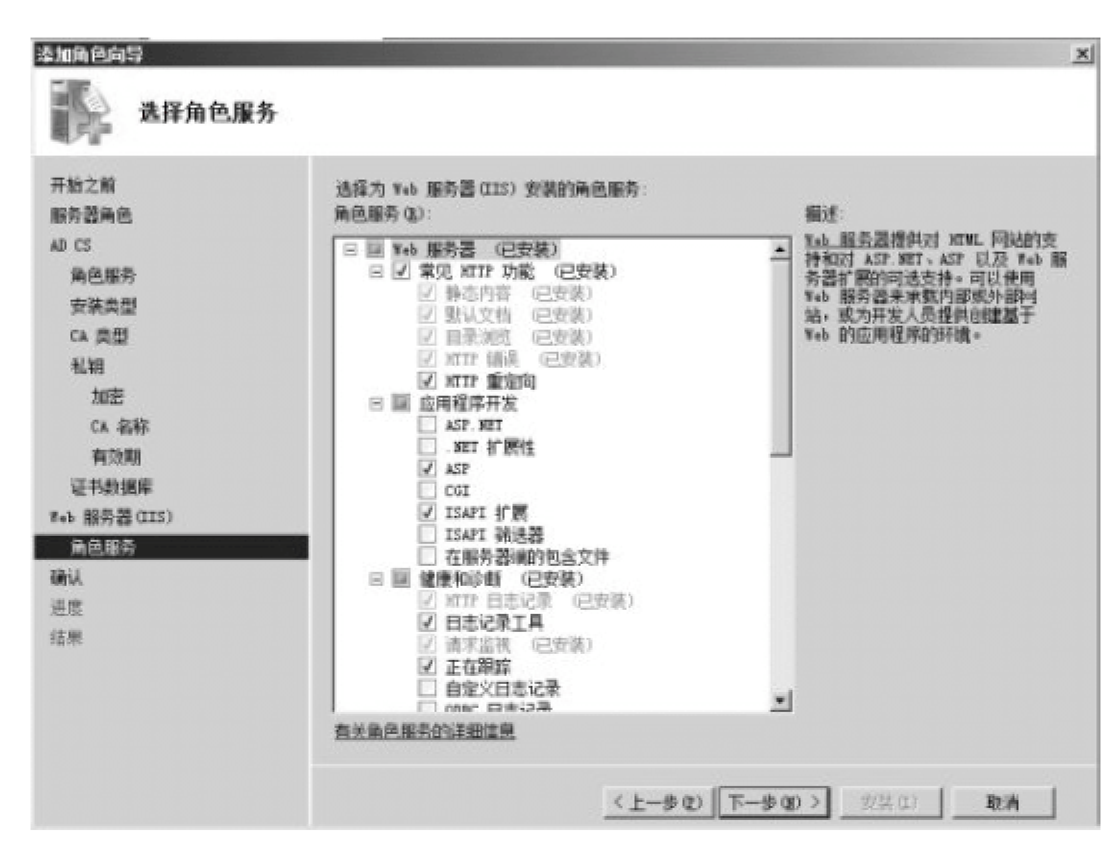


图 6-10　安装 Web 服务器所必需的角色服务

(11) 如图 6-11 所示，确认安装信息后，开始安装，单击“下一步”按钮。



图 6-11　安装进度

(12) 如图 6-12 所示，单击“下一步”按钮，安装完成。

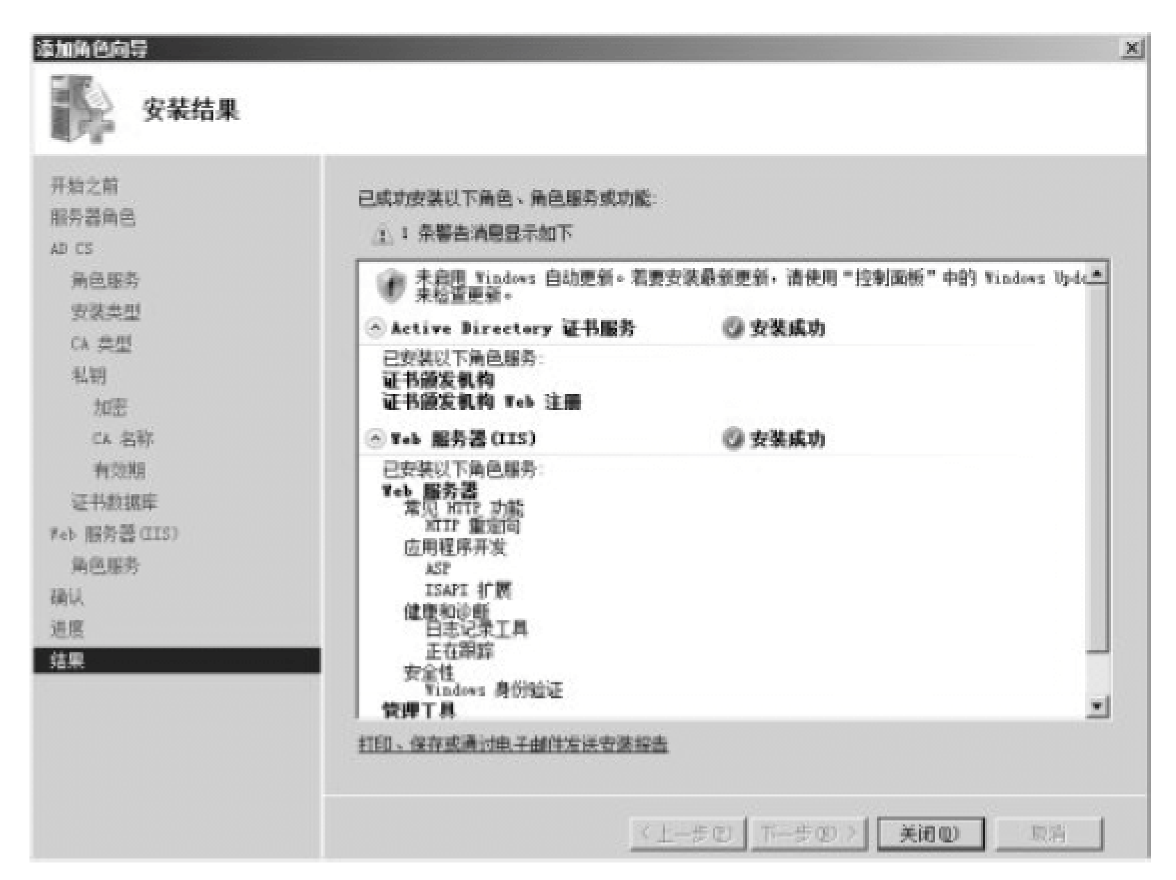


图 6-12　安装完成

(13) 安装完成后，从管理工具中可以看到“Certification Authority”，打开证书颁发机构管理器，如图 6-13 所示，在此管理证书的颁发。

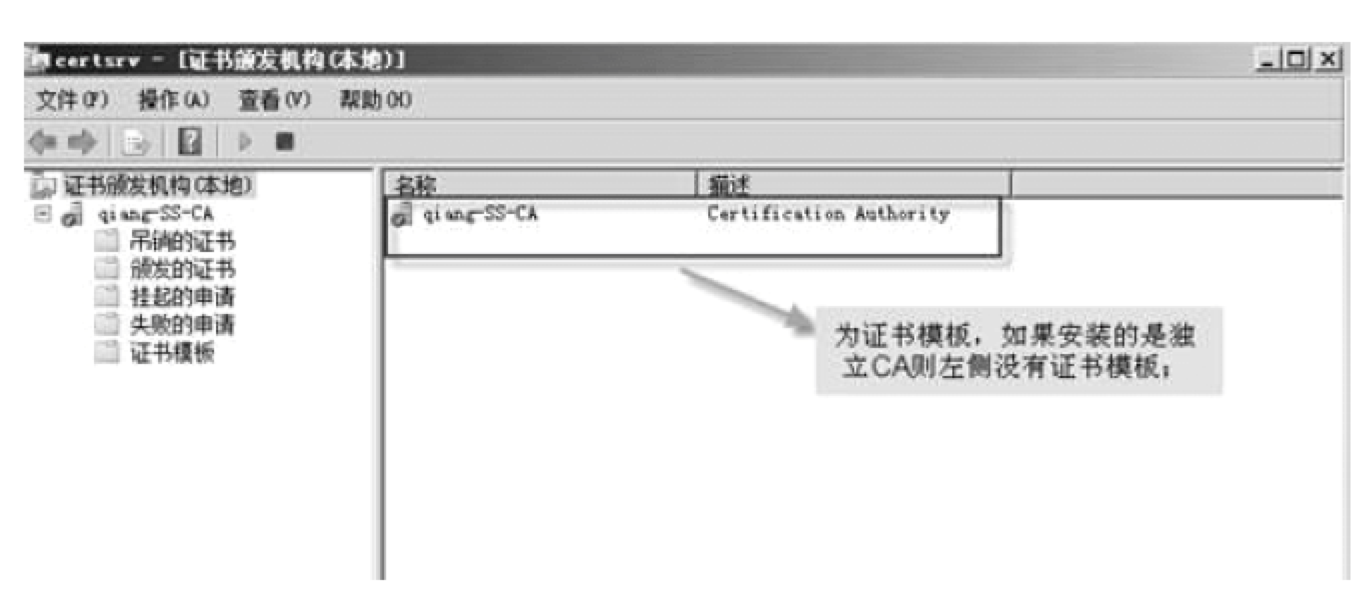


图 6-13　证书颁发机构管理器

6.2.2　证书的申请与颁发

为 Web 站点申请证书进而使用 SSL 通信协议，可以实现 Web 服务器和浏览器之间的身份认证和加密数据的传输。申请与颁发证书的步骤如下：

(1) 打开“Internet 信息服务管理器”，如图 6-14 所示，双击“证书服务器”。



图 6-14　Internet 信息服务管理器

(2) 如图 6-15 所示，单击“创建证书申请”。



图 6-15　创建证书申请

(3) 如图 6-16 所示，在“可分辨名称属性”中输入对应的信息，其中“通用名称”为站点域名或 IP 地址。单击“下一步”按钮。

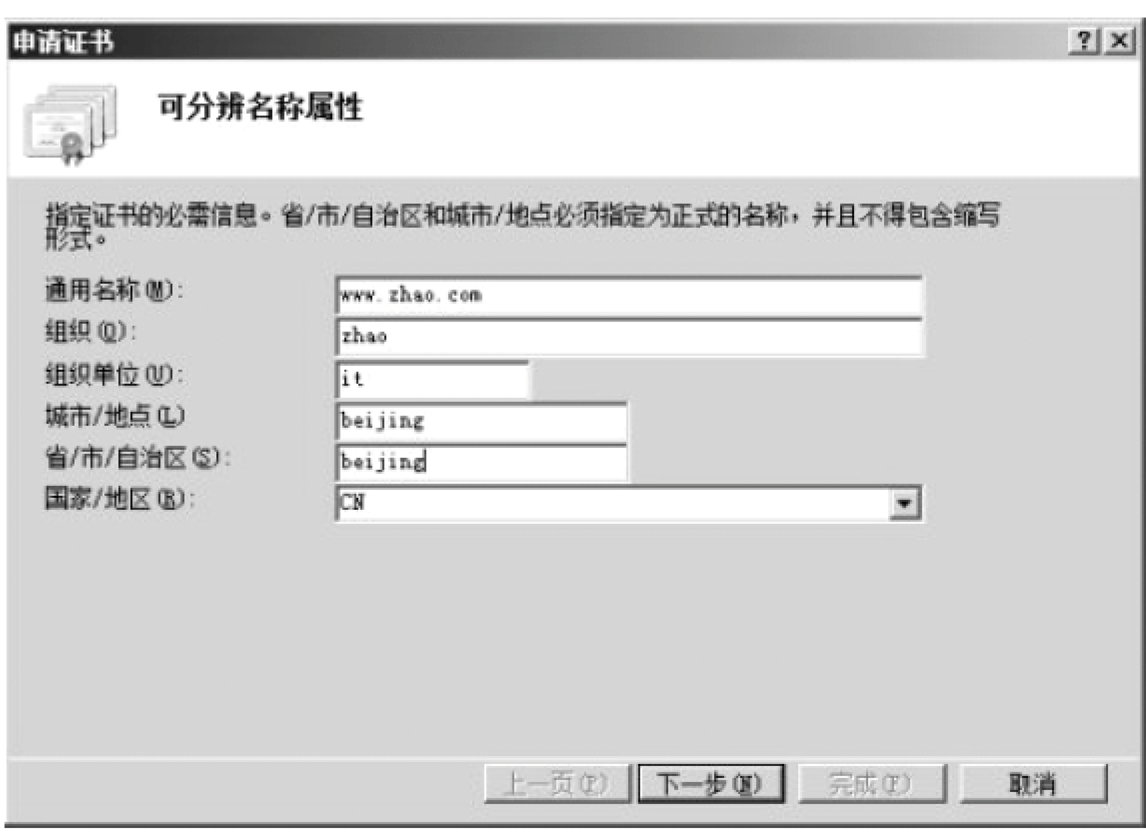


图 6-16　在“可分辨名称属性”中输入对应的信息

(4) 如图 6-17 所示，使用默认的加密程序和密钥长度即可，单击“下一步”按钮。



图 6-17　设置加密服务程序属性

(5) 如图 6-18 所示，为证书申请指定文件名和保存位置，单击“下一步”按钮。



图 6-18　为证书申请指定文件名和保存位置

(6) 完成上述步骤后，打开 c:\c.txt，如图 6-19 所示，可见证书申请文件是 Base-64 编码，复制 c.txt 中的全部内容。



图 6-19　查看、复制证书申请文件的编码

(7) 使用浏览器打开http://10.0.0.1/certsrv(10.0.0.1 为证书服务器 IP 地址)，如图 6-20 所示，单击“申请证书”。

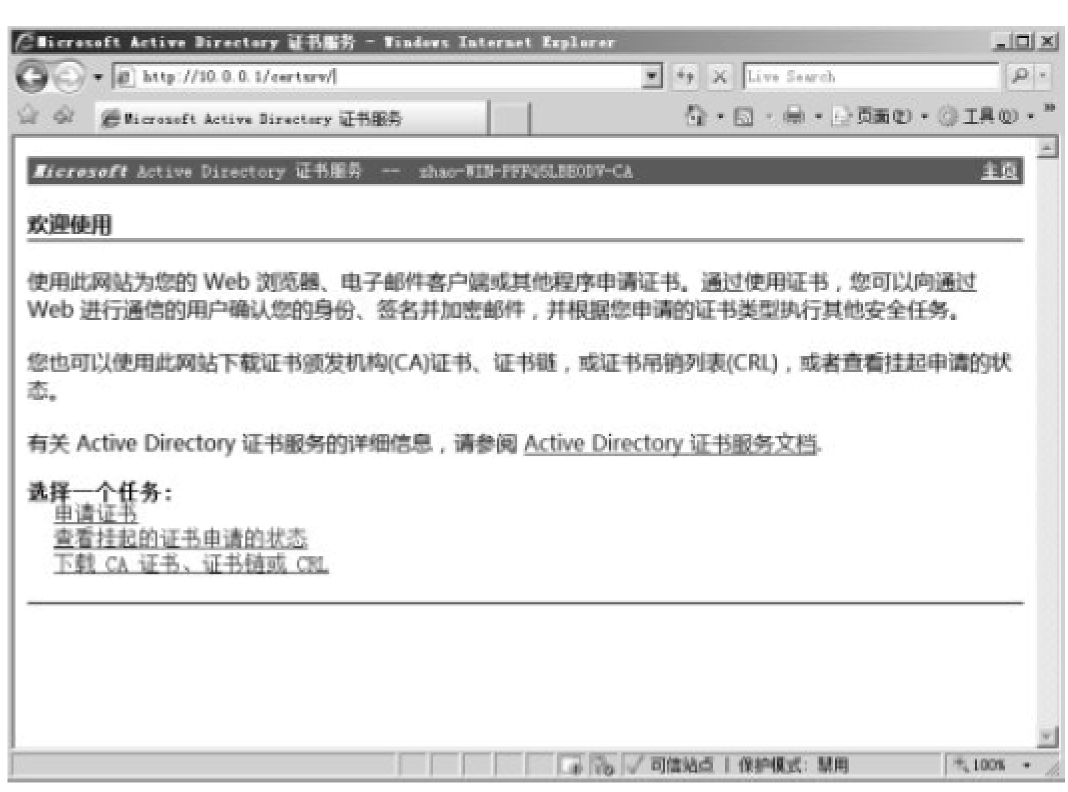


图 6-20　申请证书

(8) 如图 6-21 所示，单击“高级证书申请”。



图 6-21　高级证书申请

(9) 如图 6-22 所示，单击“使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请”。



图 6-22　选择申请方式

(10) 将 c.txt 里的内容粘贴到“Base-64 编码的证书申请”，如图 6-23 所示，证书模板选择“Web 服务器”，单击“提交”按钮。

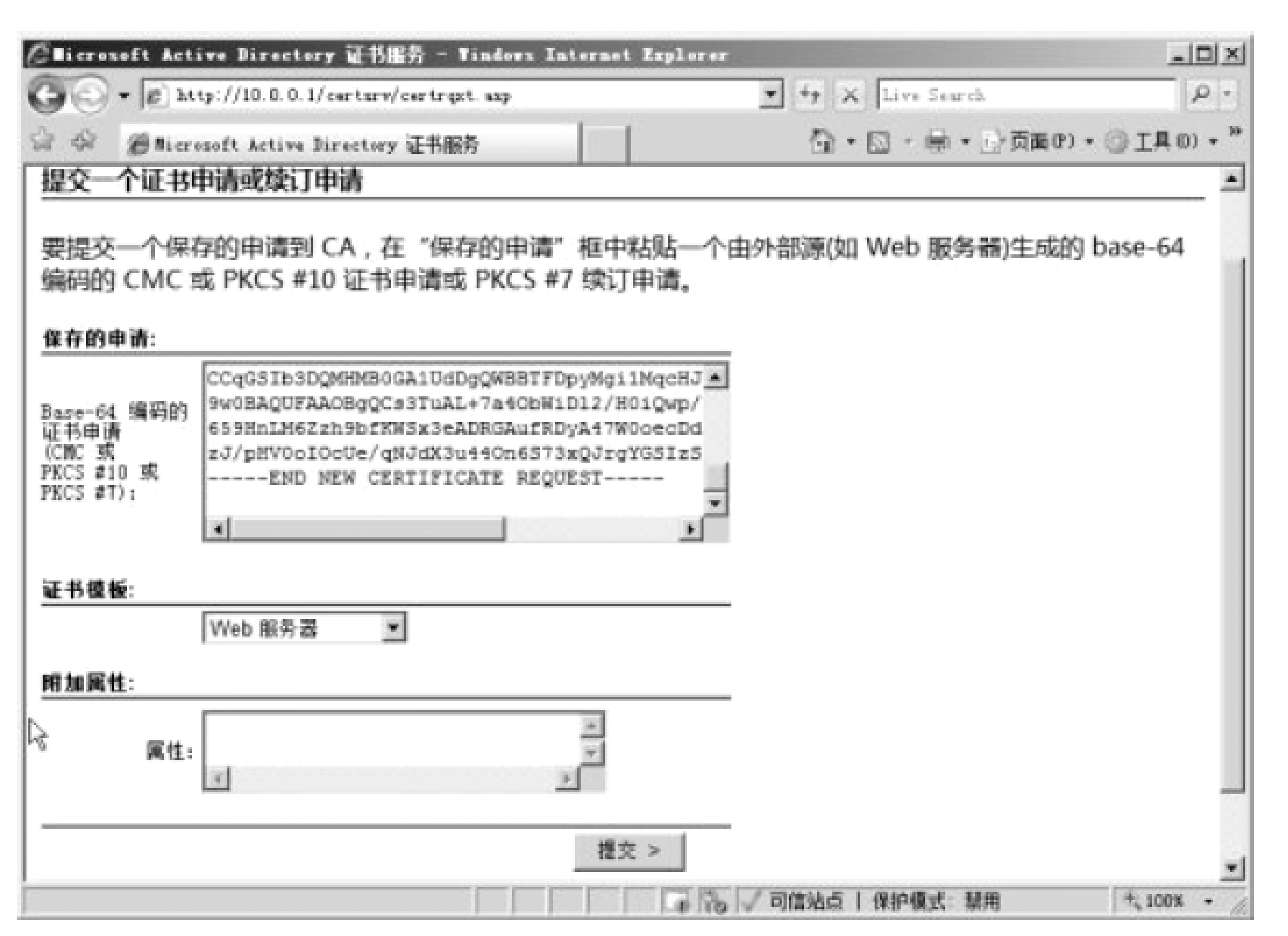


图 6-23　粘贴证书申请文件的编码

(11) 由于使用的是企业 CA，提交申请后会直接进入证书已颁发页面，如图 6-24 所示，单击“下载证书”(独立 CA 则需要管理员手动颁发证书，并重新打开第(7)步的页面，单击“下载 CA 证书”→“证书链”或“CRL”)。



图 6-24　下载 CA 证书

(12) 将证书 certnew.cer 保存到本地位置，如图 6-25 所示。

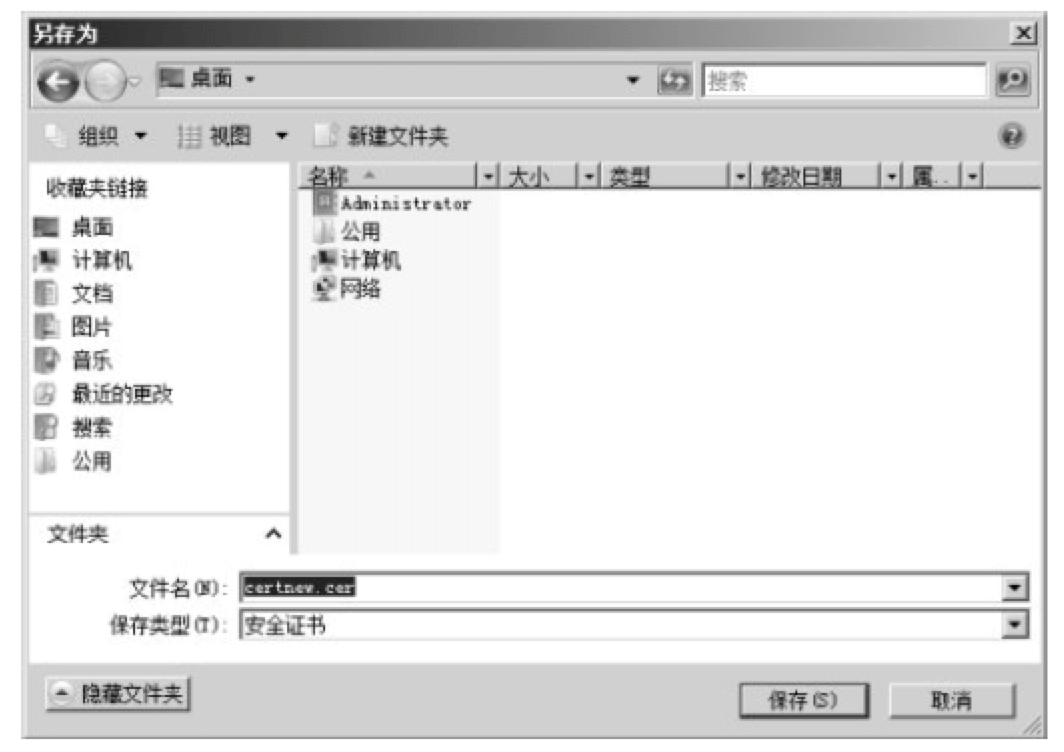


图 6-25　将证书 certnew.cer 保存到本地位置

6.2.3　安装 Web 服务器证书

操作步骤如下：

(1) 单击服务器证书中的“完成证书申请”，如图 6-26 所示。

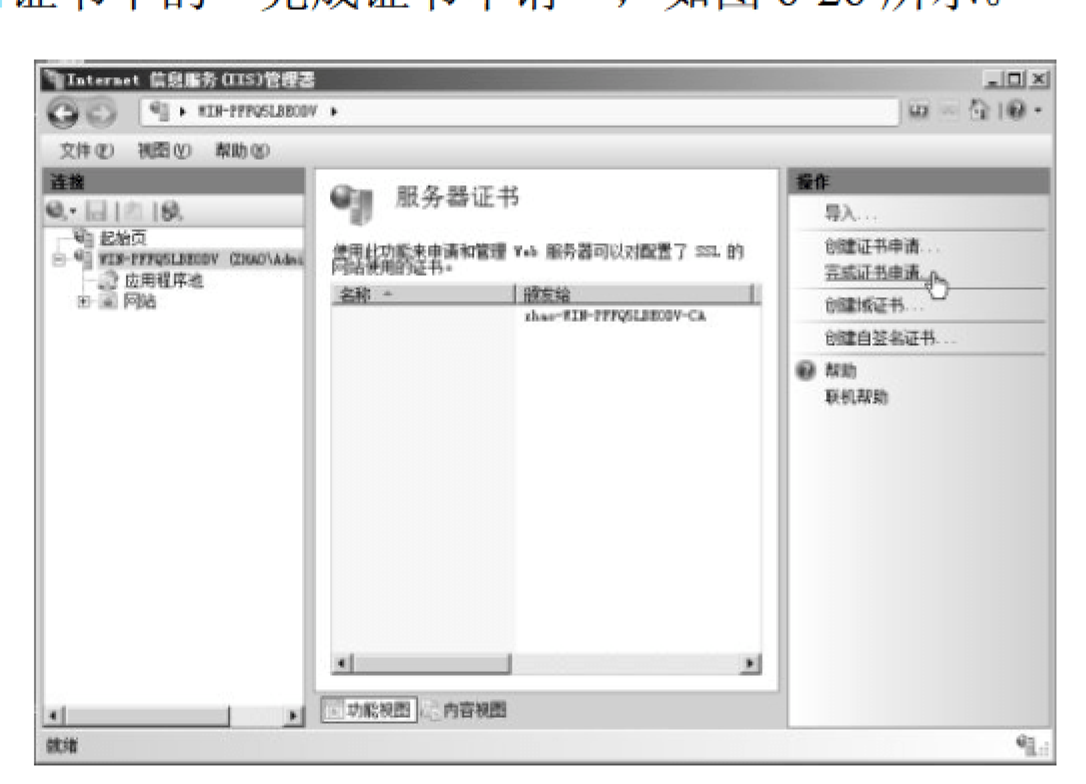


图 6-26　单击“完成证书申请”

(2) 如图 6-27 所示，选择已下载的数字证书文件 certnew.cer，并为它起一个别名，单击“确定”按钮。

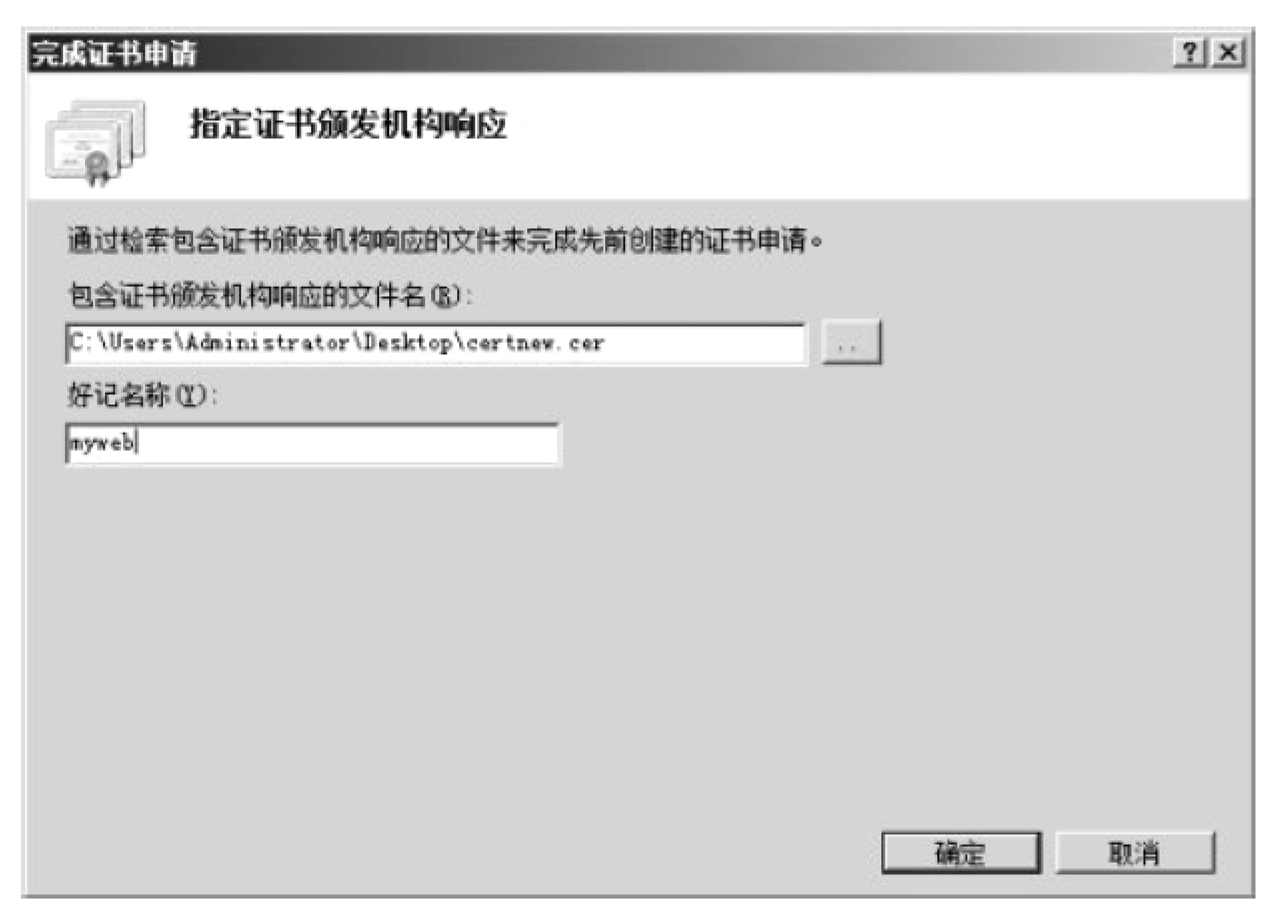


图 6-27　选择已下载的数字证书文件

6.2.4　配置安全通道(SSL)

操作步骤如下：

(1) 如图 6-28 所示，在需要启用 HTTPS 的站点上，单击“绑定”。



图 6-28　单击“绑定”

(2) 单击“添加”，添加网站绑定。如图 6-29 所示，类型选择为“https”，SSL 证书选择“myweb”，单击“确定”按钮。

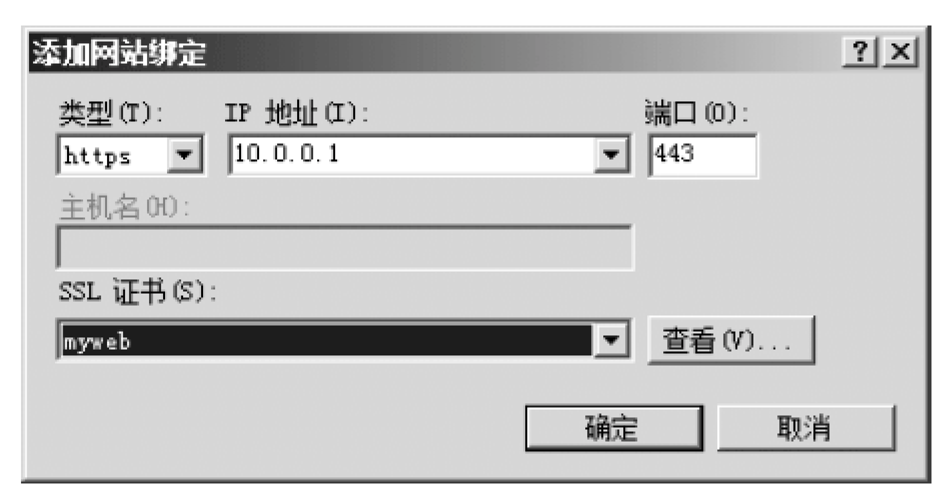


图 6-29　添加网站绑定

(3) 如图 6-30 所示，打开“SSL 设置”。



图 6-30　打开“SSL 设置”

(4) 选中“要求 SSL”和“需要 128 位 SSL”，如图 6-31 所示，单击“应用”，不管站点是否有 HTTP 类型的绑定，用户都只能以 HTTPS 方式连接站点。



图 6-31　SSL 设置并启用

经过以上步骤后，完成了配置安全通道(SSL)的任务，从而实现了基于证书的身份信息

加密和验证，较高程度地保证了网络信息传递安全。

6.3　本章小结

本章主要介绍了电子证书服务，包括电子证书的用途、证书服务器的部署、企业 CA 的安装与使用、独立根 CA 的安装与使用、证书服务的管理。正确地运用证书服务，能够大幅度地提高网络通信中的信息安全。

6.4　思考与练习

【思考题】

1. 电子证书的用途及其实现原理分别是什么?
2. 企业根 CA 与独立根 CA 的安装环境有什么区别?

【练习题】

企业 CA 的安装与使用(参考 6.2 节)、独立根 CA 的安装与使用(参考 6.3 节)。

第7章　DHCP服务

【本章导读】

动态主机配置协议能够为局域网中的客户端自动分配 IP 地址、子网掩码及其他相关的配置信息。如果网络中有可用的 DHCP 服务器，其他客户端计算机就能够自动地向其发出 DHCP 服务请求，并获取相关的 IP 配置。这种全自动的方式避免了客户端用户手工设置的麻烦和可能出现的失误，极大地降低了网络管理员的配置工作量，提高了工作效率，增强了网络管理的灵活性。通过在运行 Windows Server 2008 操作系统的计算机上添加 DHCP 服务器角色，并进行相关的参数设置，就能使该计算机成为网络中的 DHCP 服务器。

7.1　DHCP 服务概述

7.1.1　DHCP 服务简介

DHCP 是动态主机配置协议(Dynamic Host Configuration Protocol)的简称，它是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。

在 IP 网络中，每个连接 Internet 的设备都需要分配唯一的 IP 地址。地址分配有以下几种方式。

- 人工分配：即由网络管理员人工为主机设定固定的 IP 地址，且地址不会过期。
- 自动分配：作为 DHCP 客户端的主机一旦成功地从 DHCP 服务器端租用到 IP 地址之后，就永远使用这个地址。
- 动态分配：作为 DHCP 客户端的主机从 DHCP 服务器端租用到 IP 地址之后，并非永久地使用该地址，只要租约到期，客户端就得释放这个 IP 地址，以给其他主机使用。当然，客户端可以比其他主机更优先地更新租约，或是租用其他的 IP 地址。

人工分配仅适用于计算机数量较少的网络，由网络管理员为每一台主机人工设定固定 IP 地址，工作量并不大。但是如果网络中计算机数量较多或网络环境复杂多变的时候，人工分配方式就显得费时费力，而且非常容易出错。采用 DHCP 的自动分配或动态分配能够很好地解决这个问题，所有的 DHCP 客户端都能自动地获取 IP 地址、默认网关和 DNS 服务器地址等信息，从而有效避免了可能出现的输入错误，提高了工作效率。而动态分配显然又比自动分配更加灵活，尤其是当网络中的实际 IP 地址不足的时候。因为通过租约期限的控制保证 DHCP 客户端能够及时释放所占用的 IP 地址，而网络中的主机并不都是同时开机，这就使得总体上可以用较少数量的 IP 地址空间满足较多主机的需求。

DHCP 使用了租约的概念，或称为计算机 IP 地址的有效期。租用时间是不定的，主要取决于用户在某地联接 Internet 需要多久，这对于教育行业或其他用户频繁改变的环境是很实用的。通过较短的租期，DHCP 能够在一个计算机比可用 IP 地址多的环境中动态地重新配置网络。同时，DHCP 还支持为特定计算机分配静态地址，如需要永久性 IP 地址的 Web 服务器。

DHCP 服务的全过程通常分为以下 4 个阶段：

(1) DHCP 发现。DHCP 客户端在物理子网上发送广播来寻找可用的 DHCP 服务器并请求 IP 租约。该客户端生成一个目的地址为 255.255.255.255 或者一个子网广播地址的 DHCP 发现消息(通常 DHCP 消息只在本地网络传播，但是网络管理员也可以配置一个本地路由来转发 DHCP 消息给另一个子网上的 DHCP 服务器)。

(2) DHCP 提议。当 DHCP 服务器收到一个来自客户端的 DHCP 发现消息时，它会提供一个 IP 租约。DHCP 为客户保留一个 IP 地址，然后通过网络发送一个 DHCP 提议消息给客户端。该消息包含客户端的 MAC 地址、服务器提供的 IP 地址、子网掩码、租期以及提供 IP 的 DHCP 服务器的 IP 地址。

(3) DHCP 请求。当客户端收到一个 DCHP 提议时，它必须告诉所有其他的 DHCP 服务器它已经接受了一个租约提供。因此，该客户端会发送一个 DHCP 请求消息，其中包含提供租约的服务器的 IP 地址。当其他 DHCP 服务器收到了该消息后，它们会收回所有可能已提供给客户的租约。然后它们把曾经给客户保留的那个地址重新放回到可用地址池中，这样，它们就可以为其他计算机分配这个地址。任意数量的 DHCP 服务器都可以响应同一个 IP 租约请求，但是每一个客户网卡只能接受一个租约提供。

(4) DHCP 确认。当 DHCP 服务器收到来自客户的 DHCP 请求消息后，它就开始了配置过程的最后阶段。这个响应阶段包括发送一个 DHCP 确认消息给客户端。这个消息包含 IP 租约的租期和客户可能请求的其他所有配置信息。这时候，DHCP 服务过程就完成了。

7.1.2　DHCP 服务器的适用范围

通常 DHCP 适用于大型网络，然而即使在一个仅拥有少量机器的网络中，DHCP 仍然是有用的，因为一台机器可以几乎不造成任何影响地被增加到本地网络中。虽然 DHCP 有很多优势，但是在使用不当的时候，DHCP 也会造成灾难性的后果。如果 DHCP 服务器的设置有问题，将会影响网络中所有 DHCP 客户端的正常工作。如果网络中只有一台 DHCP 服务器，当它发生故障时，所有的 DHCP 客户端既无法获得 IP 地址，也无法释放已有的 IP 地址，从而导致网络通信的瘫痪。因此通常在一个重要网络中，用一组而不是一台 DHCP 服务器来管理网络参数的分配。

在 Windows 网络中，DHCP 服务器必须是一台安装有 Windows 2000 Server 或以上版本操作系统的计算机；其次，担任 DHCP 服务器的计算机还需要安装 TCP/IP 协议，并为其设置静态 IP 地址、子网掩码、默认网关等网络参数。

7.2　安装 DHCP 服务器

7.2.1　DHCP 服务器配置过程

DHCP 服务器要想正常工作，必须先经过正确的安装和配置。DHCP 服务虽然是 Windows Server 2008 系统的自带组件，但默认情况下并没有安装，需要管理员手动安装。

安装过程中或安装完毕后还需要在DHCP服务器上添加作用域，并设置作用域的名称、地址池空间、子网掩码及默认网关等信息。添加完毕后还需要激活作用域。

出于网络安全管理的考虑，如果 DHCP 服务器是域的成员，并且在安装 DHCP 服务过程中没有选择授权，那么在安装完成后不能直接使用。DCHP 服务器必须先进行授权，然后才能为 DHCP 客户端提供 DHCP 服务(独立服务器是不需要授权的)。

出于数据安全的考虑，网络管理员还应该对 DHCP 服务器定期进行备份，以便在需要的时候还原 DHCP 服务器设置，保证网络的稳定运行。

7.2.2　安装 DHCP 服务器

在 Windows Server 2008 系统中安装“DHCP 服务器”可以通过添加角色向导完成，具体步骤如下：

(1) 通过单击“服务器管理器”中的“添加角色”链接启动“添加角色向导”，在“选择服务器角色”步骤所显示的角色列表中选中“DHCP 服务器”复选框，如图 7-1 所示，然后单击“下一步”按钮。

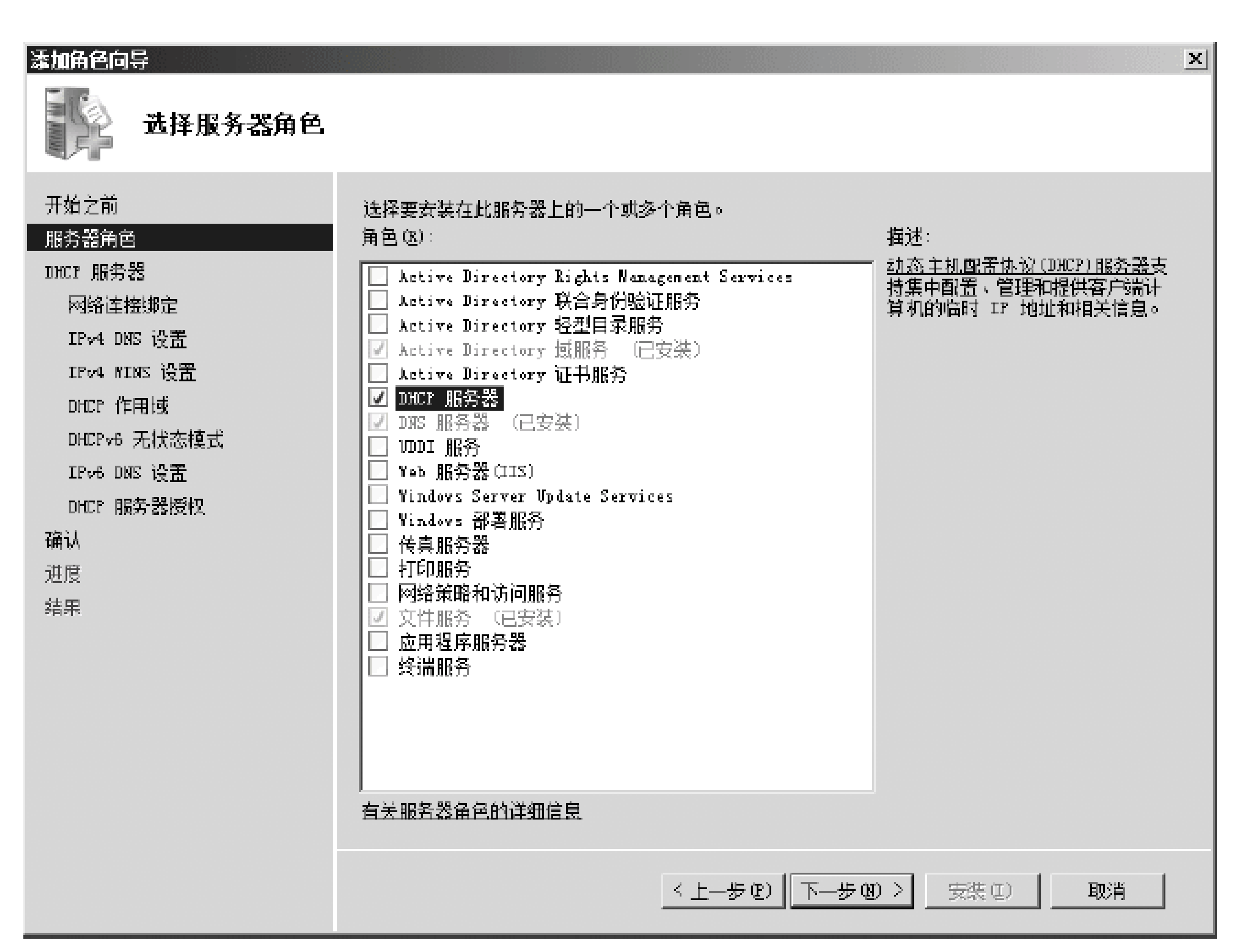


图 7-1　添加角色向导-选中 DHCP 服务器角色

(2) 接下来的页面会显示 DHCP 服务器的简介信息和安装 DHCP 服务器的注意事项，单击“下一步”按钮，将进入如图 7-2 所示的“选择网络连接绑定”步骤。在此步骤中会自动列出该服务器现有的具备固定 IP 地址的网络连接，并显示出该连接的名称、所使用的网卡类型及 MAC 地址。如果该服务器拥有多个具有静态 IP 地址的网络连接，则每个网络连接都可用于为单独子网上的 DHCP 客户端提供服务。

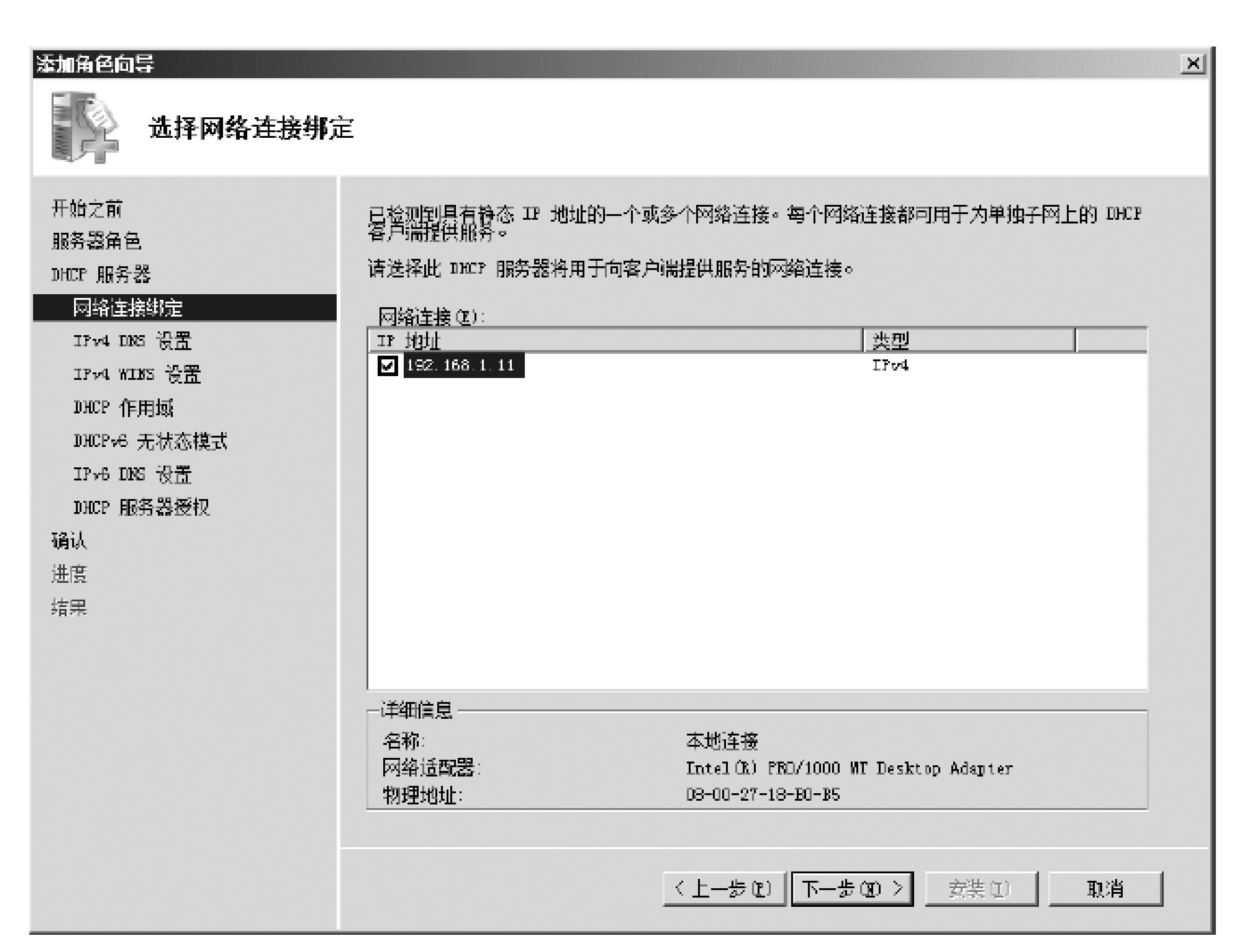


图 7-2　添加角色向导-选择网络连接绑定

(3) 下一步将指定与 DHCP 服务器相关的 DNS 服务器设置，如图 7-3 所示，如果 DHCP 服务器处于某个域中，系统会自动把该域的名称和域中的 DNS 服务器地址填入相应的编辑框中。

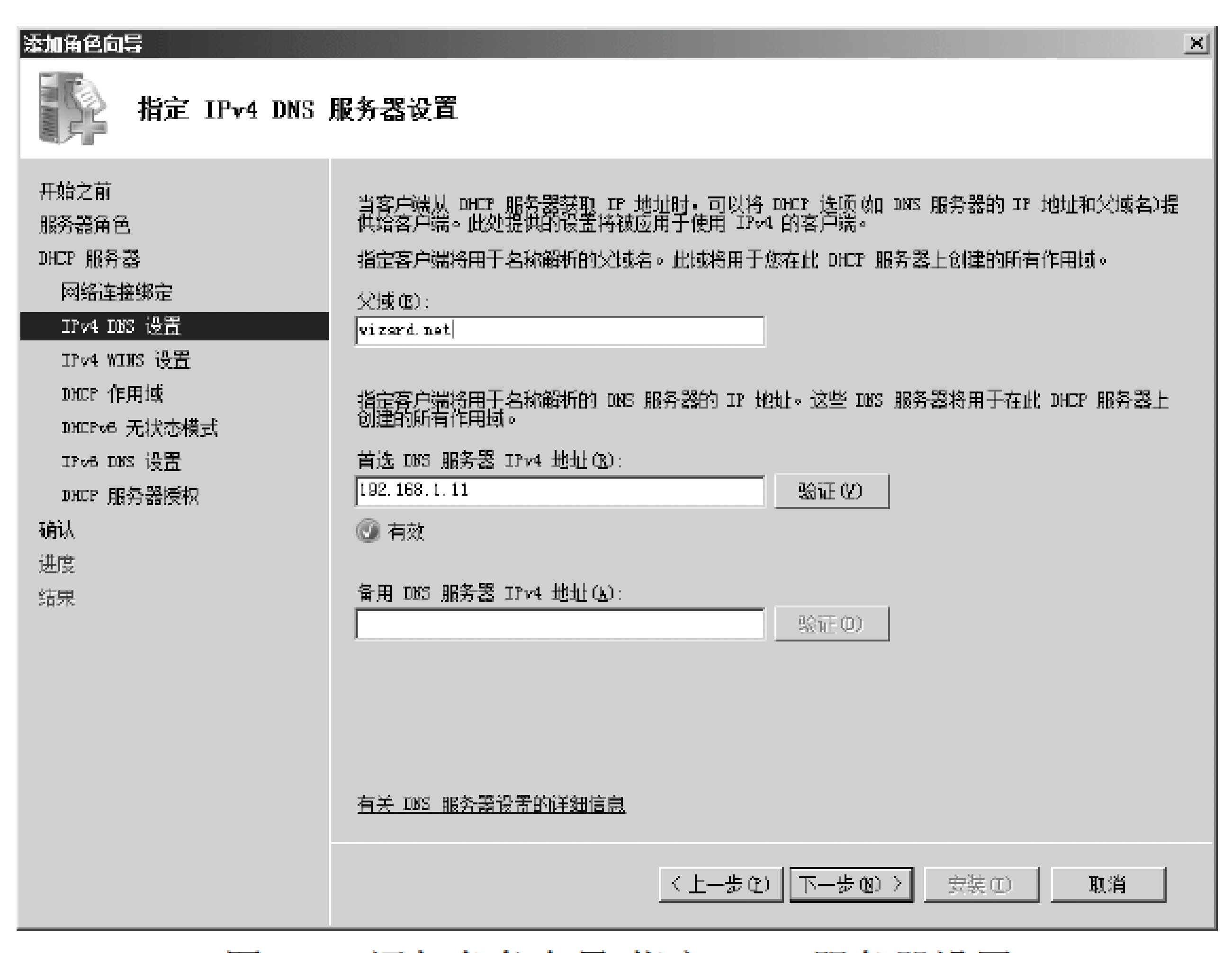


图 7-3　添加角色向导-指定 DNS 服务器设置

(4) 下一步骤是指定 WINS 服务器设置，如图 7-4 所示。WINS 服务主要支持运行旧

版 Windows 的客户端和使用 NetBIOS 名称的应用程序。如果网络中的所有主机都运行 Windows 2000 或 Windows XP 及更高版本的操作系统，并且网络中没有任何需要 NetBIOS 名称的应用程序，如旧版的 Exchange Server 或 BackOffice 等，则应选择“不需要 WINS”。

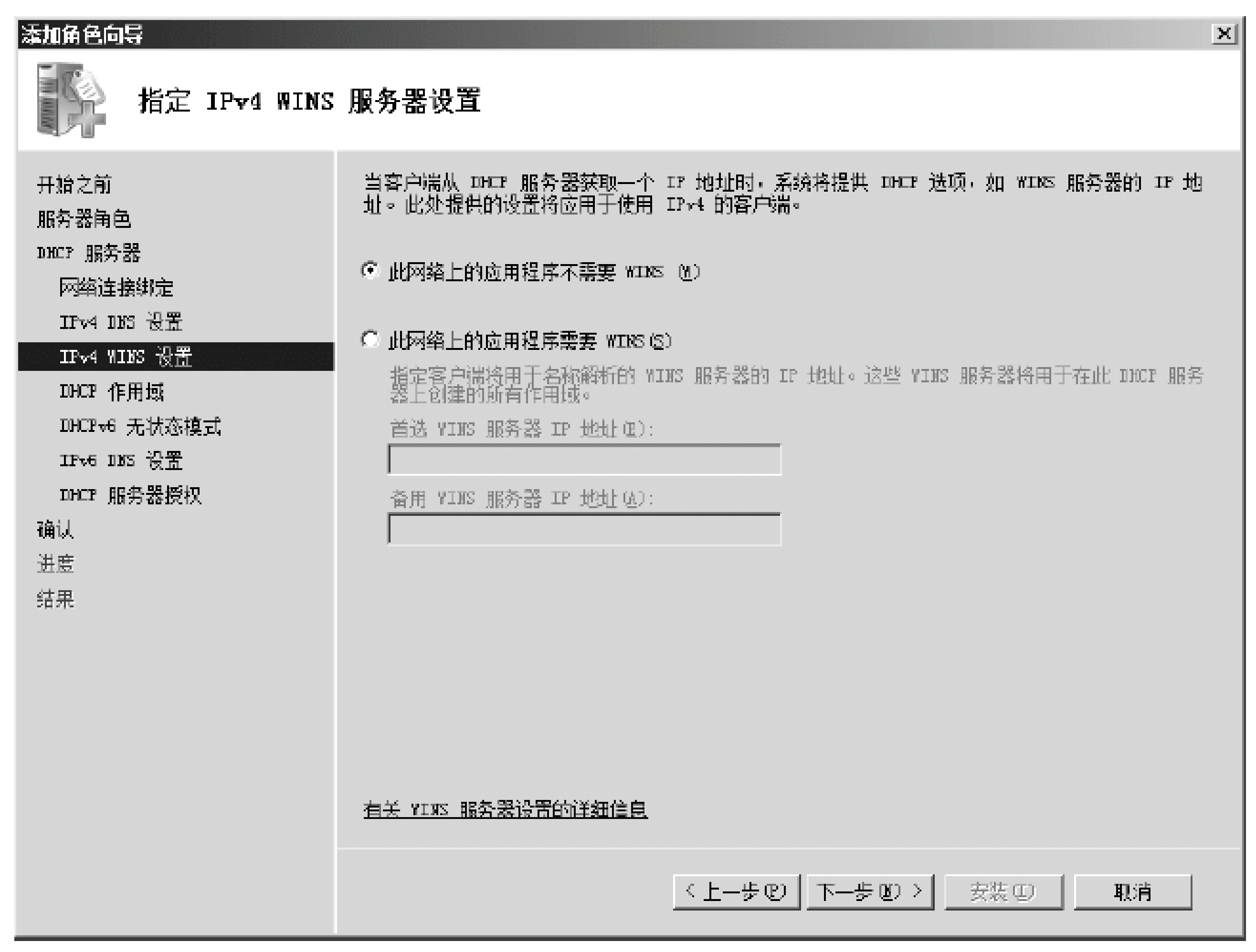


图 7-4　添加角色向导-指定 WINS 服务器设置

(5) 接下来是“添加或编辑 DHCP 作用域”步骤，如图 7-5 所示，DHCP 作用域是为了便于管理而对子网上使用 DHCP 服务的计算机 IP 地址进行的分组，由给定子网上 DHCP 服务器可以租用给客户端的 IP 地址池组成，例如子网 192.168.1.0 中从地址 192.168.1.100 到地址 192.168.1.200 的地址池。在此步骤中，管理员可以通过单击“添加”按钮打开如图 7-6 所示的“添加作用域”对话框，输入相关参数完成新作用域的添加。

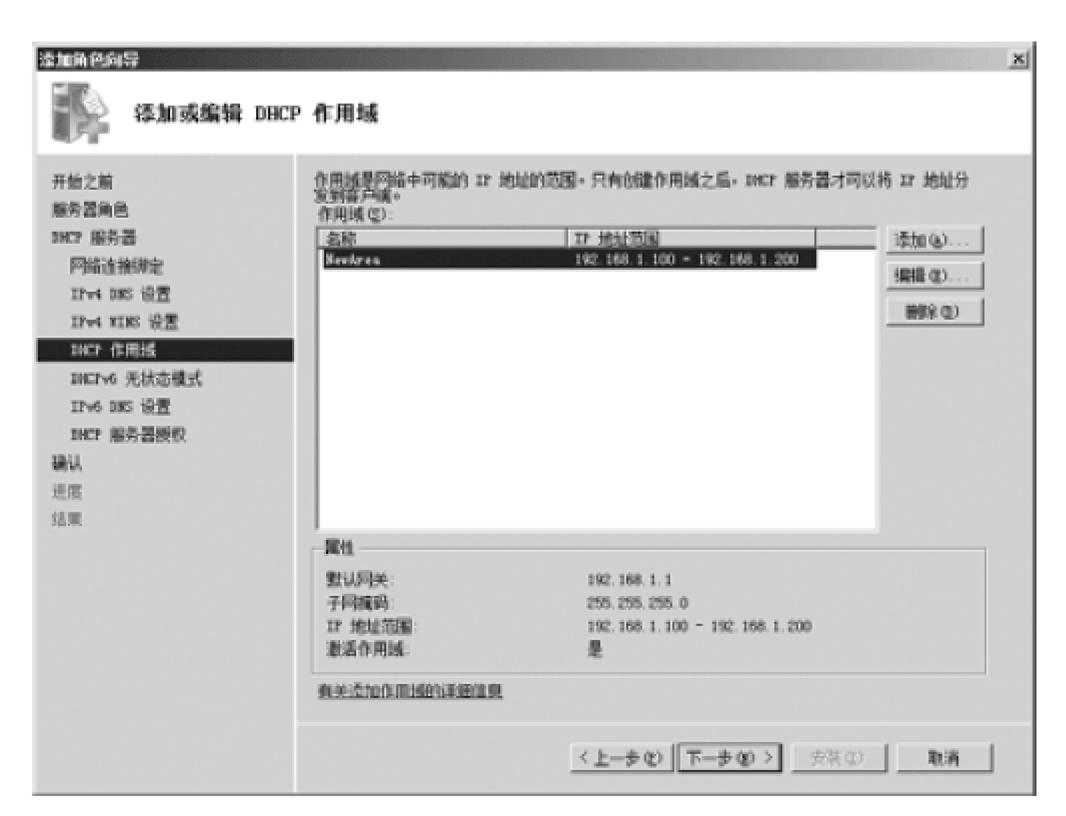



图 7-5　添加角色向导-添加或编辑 DHCP 作用域

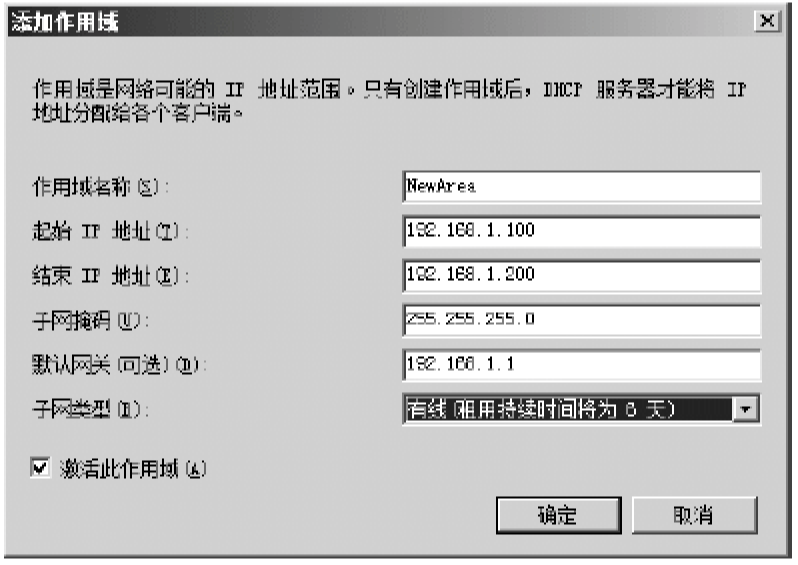


图 7-6　“添加作用域”对话框

(6) 下一步骤是配置 DHCPv6 无状态模式，如图 7-7 所示，由于目前不需配置 IPv6，因此选中“对此服务器禁用 DHCPv6 无状态模式”单选按钮。

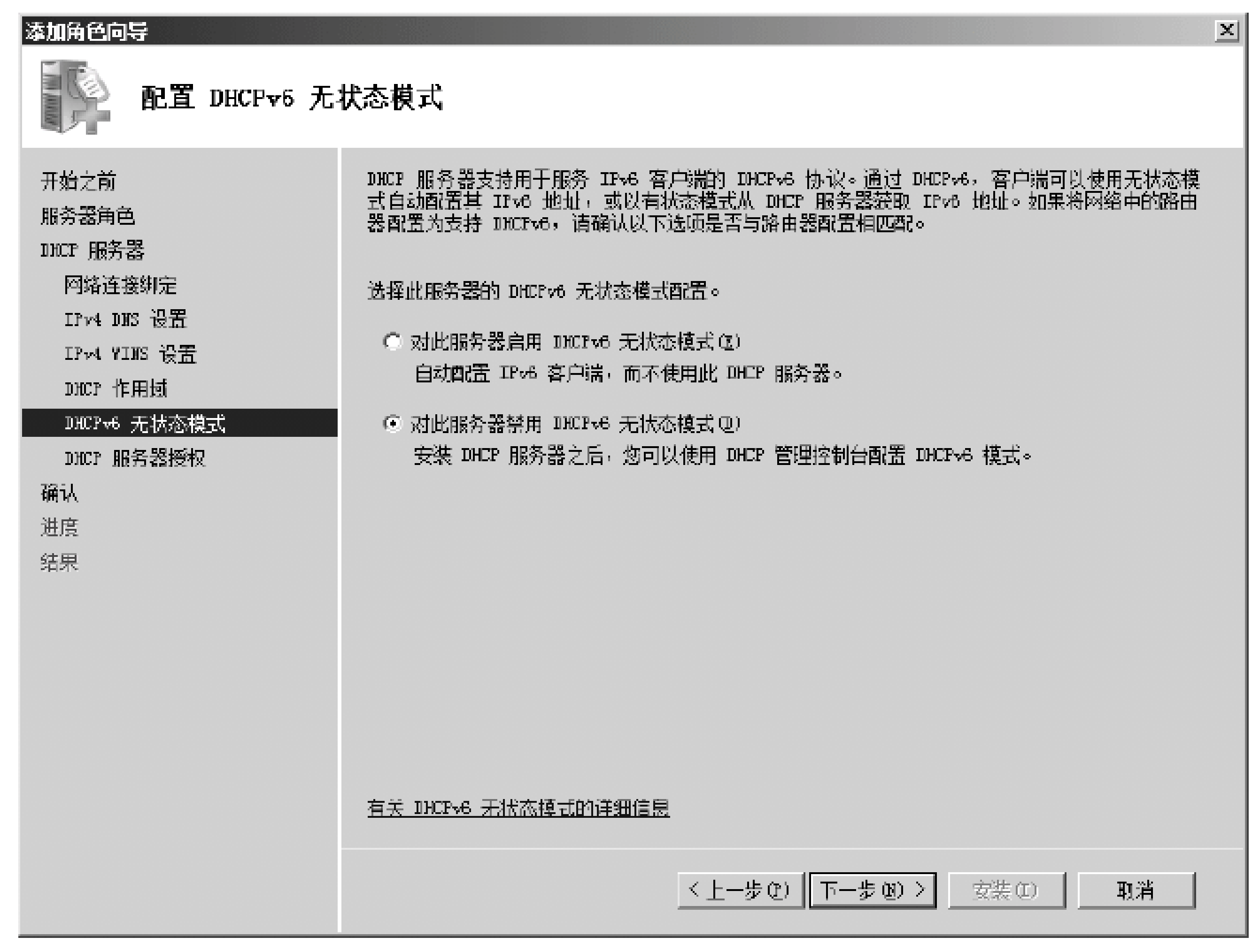


图 7-7　添加角色向导-配置 DHCPv6 无状态模式

(7) 接下来是“授权 DHCP 服务器”步骤，如图 7-8 所示，在此可以选择“使用当前凭据”以当前登录帐户授权，也可以选择“使用备份凭据”使用其他帐户授权。如果想对 DHCP 服务器暂不授权，可以选择“跳过 AD DS 中此 DHCP 服务器的授权”，以后再根据需要在 DCHP 控制台中进行授权操作。

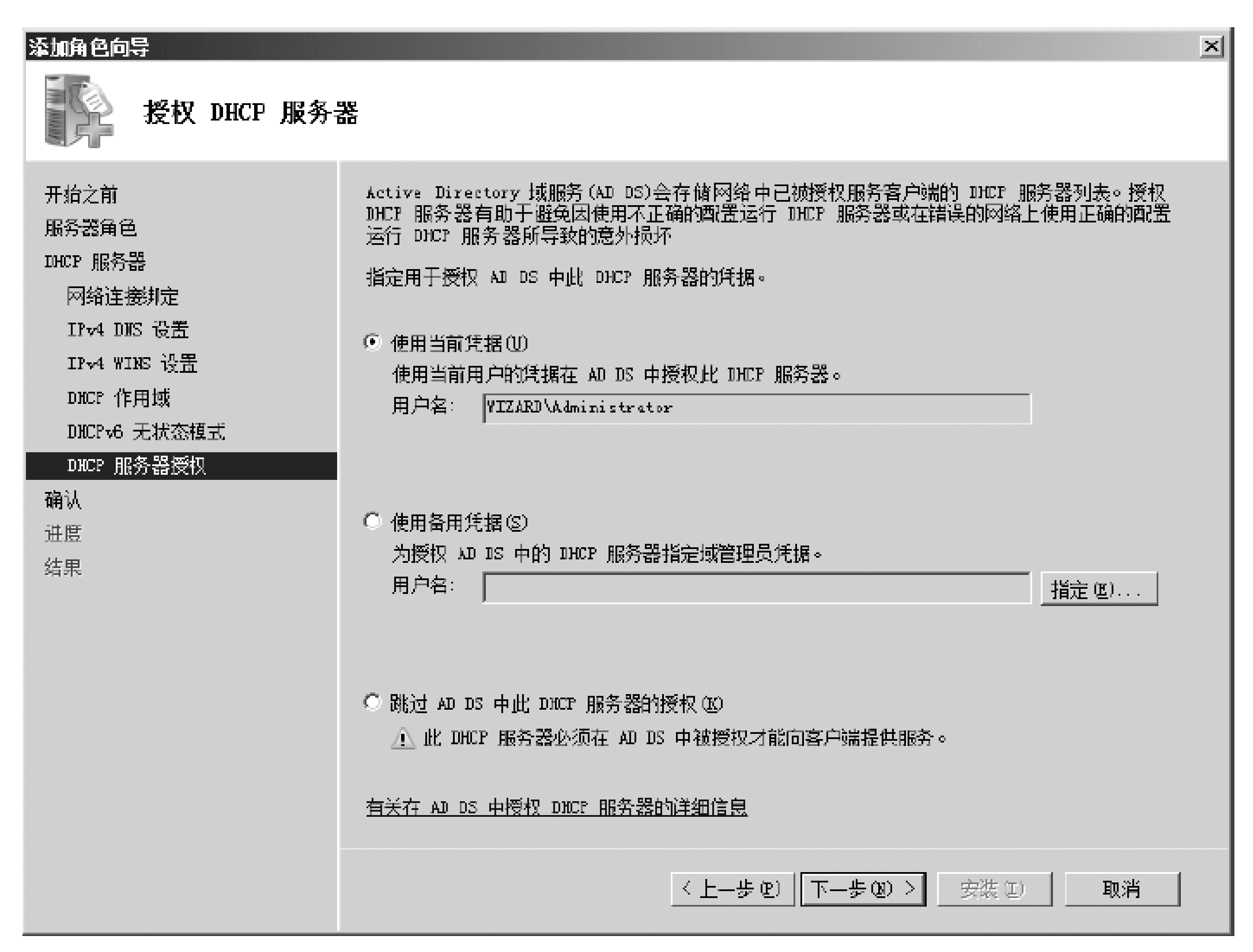


图 7-8　添加角色向导-授权 DHCP 服务器

(8) 最后显示“确认安装选择”，如图 7-9 所示，列出前面各步骤中所做的配置信息，如需更改，可通过“上一步”按钮或窗口左侧的步骤链接返回某个步骤进行修改。如果无需更改，则可单击“安装”按钮开始安装 DHCP 服务器。

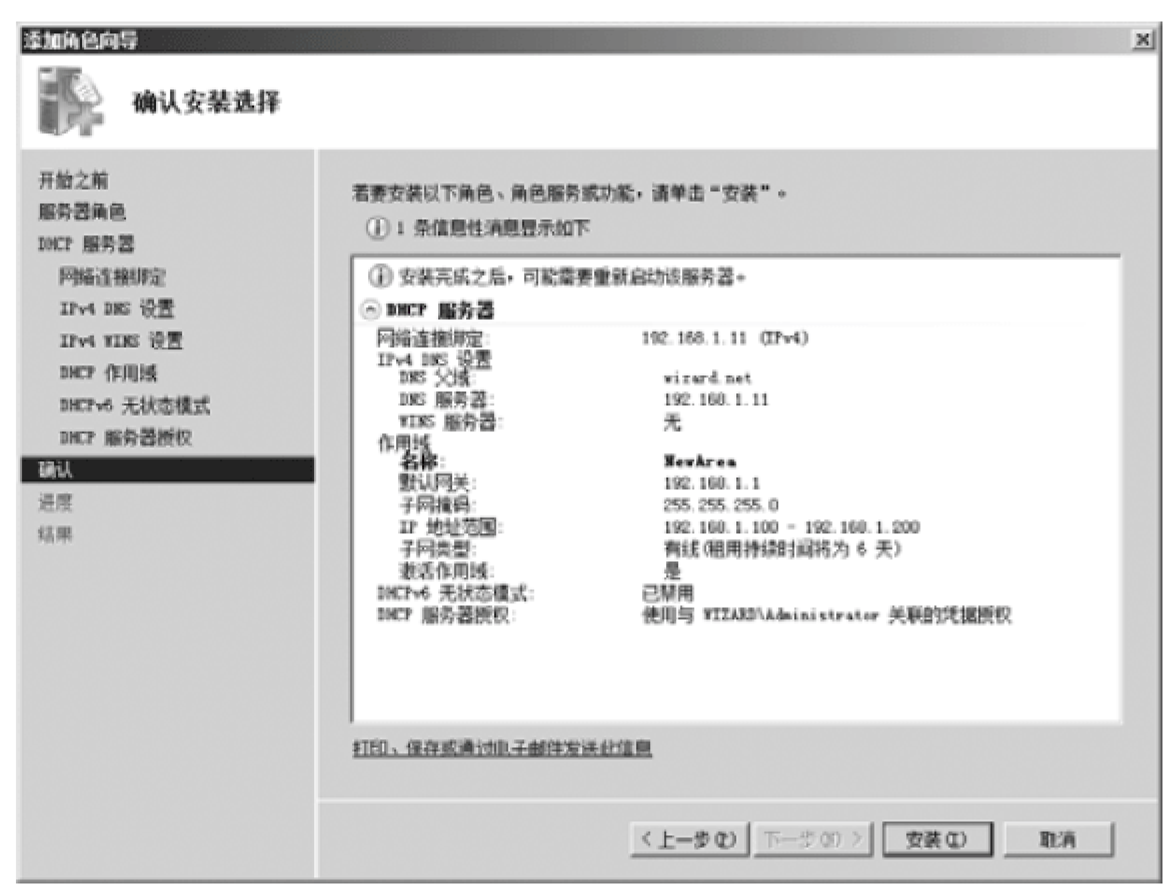


图 7-9　添加角色向导-确认安装选择

(9) 经过一定时间的安装后，系统会显示“安装结果”信息，如图 7-10 所示，提示 DHCP 服务器已经安装成功。此时单击“关闭”按钮关闭“添加角色向导”，完成整个安装过程。



图 7-10　添加角色向导-安装结果

7.2.3　为 DHCP 服务器授权

为避免因使用不正确的配置运行 DHCP 服务器，或者在错误的网络上使用正确的配置运行 DHCP 服务器所导致的意外损坏，Windows Server 2008 规定凡在域中安装的 DHCP 服务器必须经过授权才能向客户端提供 DHCP 服务。如果在安装 DHCP 服务器的时候没有授权，则在安装完成后必须通过 DHCP 控制台对其进行授权。

打开“管理工具”中的 DHCP 控制台，在左侧树形列表中右击 DHCP 服务器的名称，在弹出的快捷菜单中选择“授权”命令，即可为 DHCP 服务器授权。如图 7-11 所示即是已经过授权并添加了作用域的 DHCP 服务器的情况。

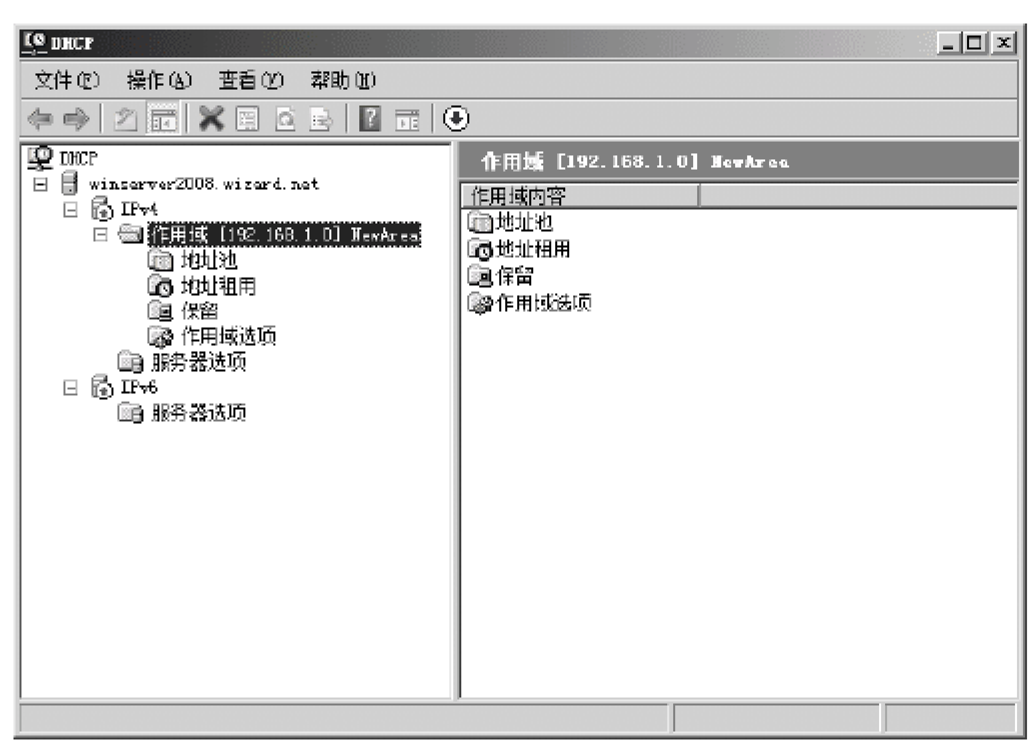


图 7-11　DHCP 控制台

7.3　DHCP 服务器的设置

7.3.1　DHCP 选项的设置

在为 DHCP 客户端设置了基本的 TCP/IP 配置如 IP 地址、子网掩码和默认网关之后，大多数客户端还需要 DHCP 服务器通过 DHCP 选项提供其他信息。其中最常见的信息如下：

- 路由器。DHCP 客户端所在子网上路由器的 IP 地址首选列表。客户端可根据需要与这些路由器联系以转发目标为远程主机的 IP 数据包。
- DNS 服务器。可由 DHCP 客户端用于解析域主机名称查询的 DNS 名称服务器的 IP 地址。
- DNS 域。指定 DHCP 客户端在 DNS 域名称解析期间解析不合格名称时应使用的域名。
- WINS 节点类型。供 DHCP 客户端使用的首选 NetBIOS 名称解析方法，如仅用于广播的 B 节点或用于点对点和广播混合模式的 H 节点。
- WINS 服务器。供 DHCP 客户端使用的主要和辅助 WINS 服务器的 IP 地址。

在一个客户端主机数量众多、类型各异、功能不同的复杂网络结构中，同一台 DHCP 服务器需要面对不同的 DHCP 客户端，并根据它们的类别和需求，分别指派不同的 DHCP 选项设置。为了能够灵活准确地完成上述工作，DHCP 服务器允许管理员从以下几个不同的级别管理 DHCP 选项：

- 预定义选项。在这一级，管理员可以控制为 DHCP 服务器预定义哪些类型的选项，以便作为可用选项显示在任何一个通过 DHCP 控制台提供的选项配置对话框，如“服务器选项”、“作用域选项”或“保留选项”中。可根据需要将选项添加到标准选项预定义列表或从该列表中删除选项。设置预定义选项的方法是在 DHCP 控制台中的 DHCP 服务器上右击，在弹出的快捷菜单中选择“设置预定义的选项”

命令，如图 7-12 所示，打开“预定义的选项和值”对话框，如图 7-13 所示。在这里可以查看现有的选项类别，还可通过单击“添加”按钮打开“选项类型”对话框，添加新的选项。



图 7-12　DHCP 控制台-设置预定义的选项



图 7-13　DHCP 控制台-预定义的选项和值

- 服务器选项。在此赋值的选项默认应用于 DHCP 服务器中的所有作用域和客户端或由它们默认继承。此处配置的选项值可以被其他值覆盖，但前提是在作用域选项、保留选项、类别选项级别上设置这些值。“服务器选项”在 DHCP 服务器安装后即存在，在这个选项上右击，在弹出的快捷菜单中选择“配置选项”命令，即可打开如图 7-14 所示的“服务器选项”对话框。在其中可配置在 DHCP 控制台中显示的服务器选项。



图 7-14　DHCP 控制台-服务器选项

- 作用域选项。在此赋值的选项仅应用于 DHCP 控制台树中选定的相应作用域中的客户端。此处配置的选项值可以被其他值覆盖，但前提是在保留选项或类别选项级别上设置这些值。同样，“作用域选项”在 DHCP 服务器作用域创建后即存在，在这个选项上右击，在弹出的快捷菜单中选择“配置选项”命令，即可打开如图 7-15 所示的“作用域选项”对话框。在其中可配置在 DHCP 控制台中显示的作用域选项。



图 7-15　DHCP 控制台-作用域选项

- 保留选项。为那些仅应用于特定的 DHCP 保留客户端的选项赋值。要使用该级别的指派，必须首先为相应客户端在向其提供 IP 地址的相应 DHCP 服务器和作用域中添加保留。这些选项为作用域中使用地址保留配置的单独 DHCP 客户端而设置。只有在客户端上手动配置的属性才能替代在该级别指派的选项。
- 类别选项。主要是针对客户端将自己设置为某些特定类别的设置选项，类别选项就是用来识别客户端标识的类别。设置类别可以通过在 DHCP 控制台中的 DHCP 服务器上右击，在弹出的快捷菜单中选择“定义用户类别”命令，弹出如图 7-16 所示的“DHCP 用户类别”对话框，然后单击“添加”按钮，在弹出的“新建类别”对话框中输入新建类别的名称、相关描述及名称的二进制编码信息，如图 7-17 所示，以建立需要的用户类别。

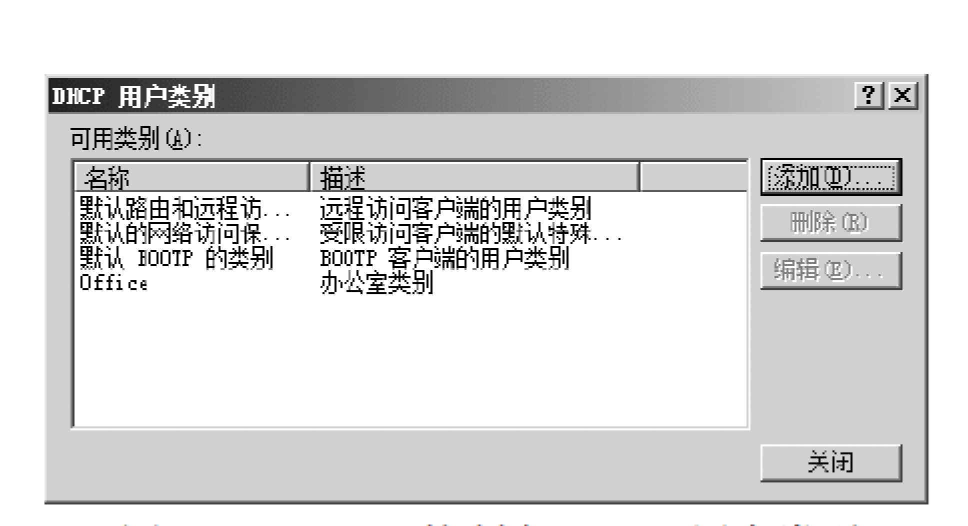


图 7-16　DHCP 控制台-DHCP 用户类别

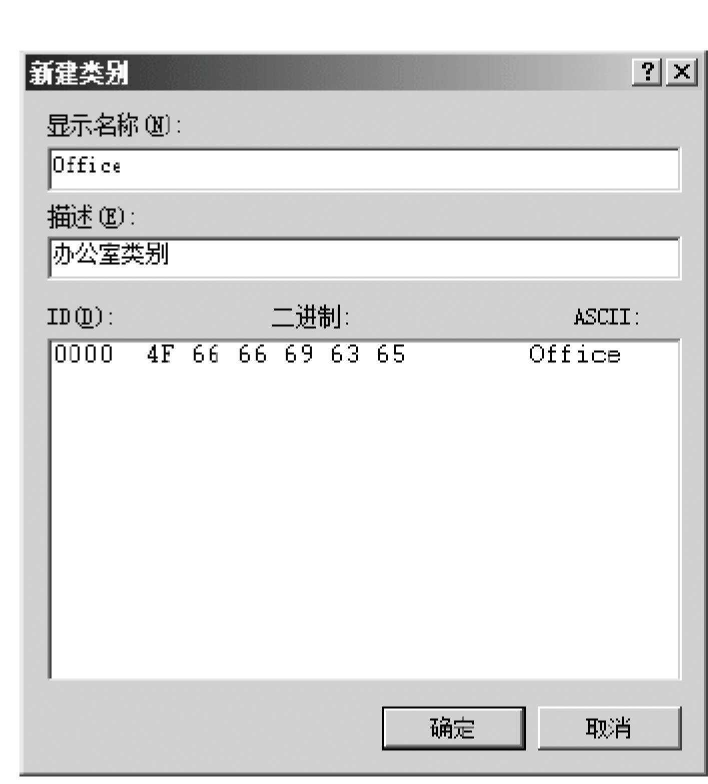


图 7-17　DHCP 控制台-新建类别

建立用户类别后，即可在使用任何选项配置对话框(配置服务器选项、作用域选项或新建保留)时，通过单击打开“高级”选项卡来配置和启用标识，为指定用户或供应商类别的成员客户端的指派选项。根据所处的环境，只有那些根据所选类别标识自己的 DHCP 客户端才能分配到网络管理员为该类别明确配置的选项数据。

当服务器选项、作用域选项、保留选项与类别选项的设置有冲突时，默认最高的优先级别是类别选项，然后是保留选项，接下来是作用域选项，最后是服务器选项。也就是说

服务器选项的优先级别最低。如果客户端计算机上有手动设置，那么客户端的设置优先级别将高于 DHCP 服务器上的所有设置。

7.3.2　新建作用域

为了向网络中的计算机提供 DHCP 服务，必须创建作用域。为了向不同网络中的客户端提供不同的 IP 地址和相关信息，还需要创建不同的作用域。因此一个 DHCP 服务器中可以有多个不同的作用域。既可以在安装 DHCP 服务器的时候添加和设置作用域，也可以在以后根据需要随时建立新的作用域。新建作用域的基本步骤如下：

(1) 在 DHCP 控制台中的 DHCP 服务器上右击，在弹出的快捷菜单中选择“新建作用域”命令，即可弹出“新建作用域向导”对话框，如图 7-18 所示。

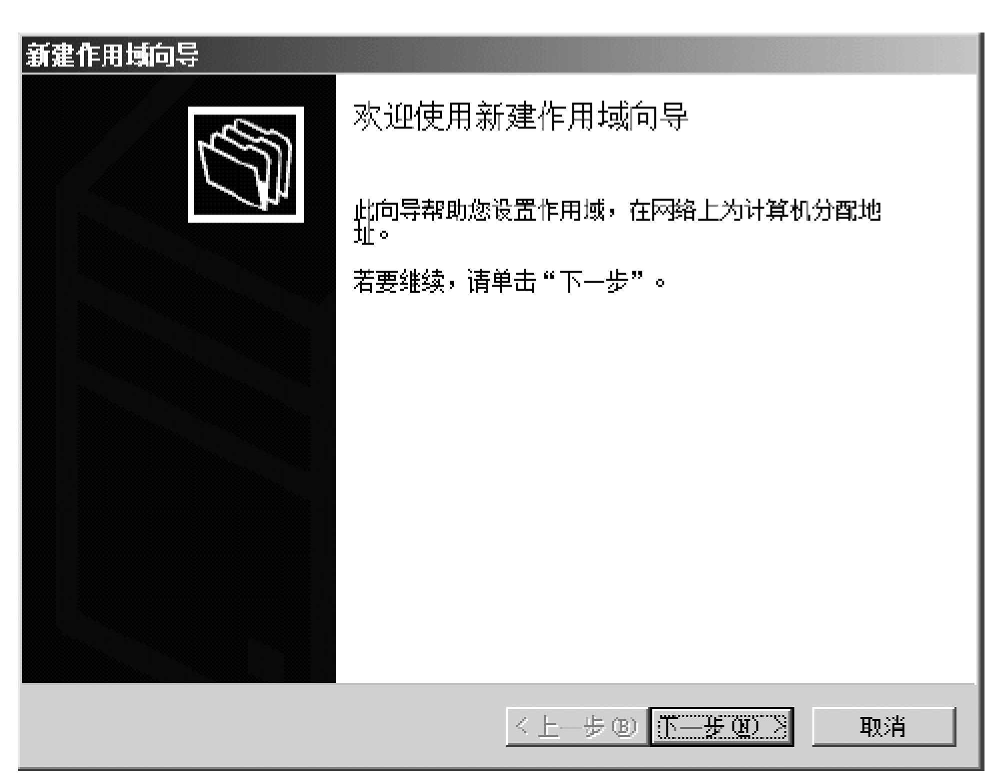


图 7-18　“新建作用域向导”对话框

(2) 向导中的第一步就是输入新作用域的名称及其相关的描述信息，如图 7-19 所示。

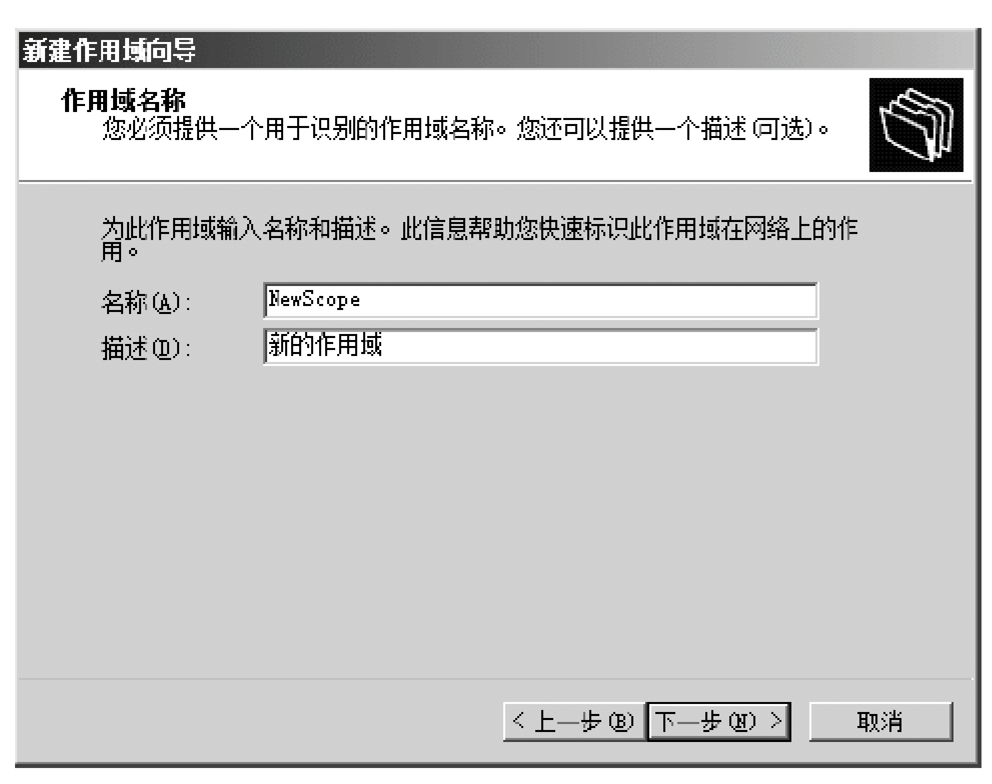


图 7-19　新建作用域向导-作用域名称

(3) 第二步是指定新作用域所包含的地址范围，以及对应的子网掩码长度或值，如图 7-20 所示。

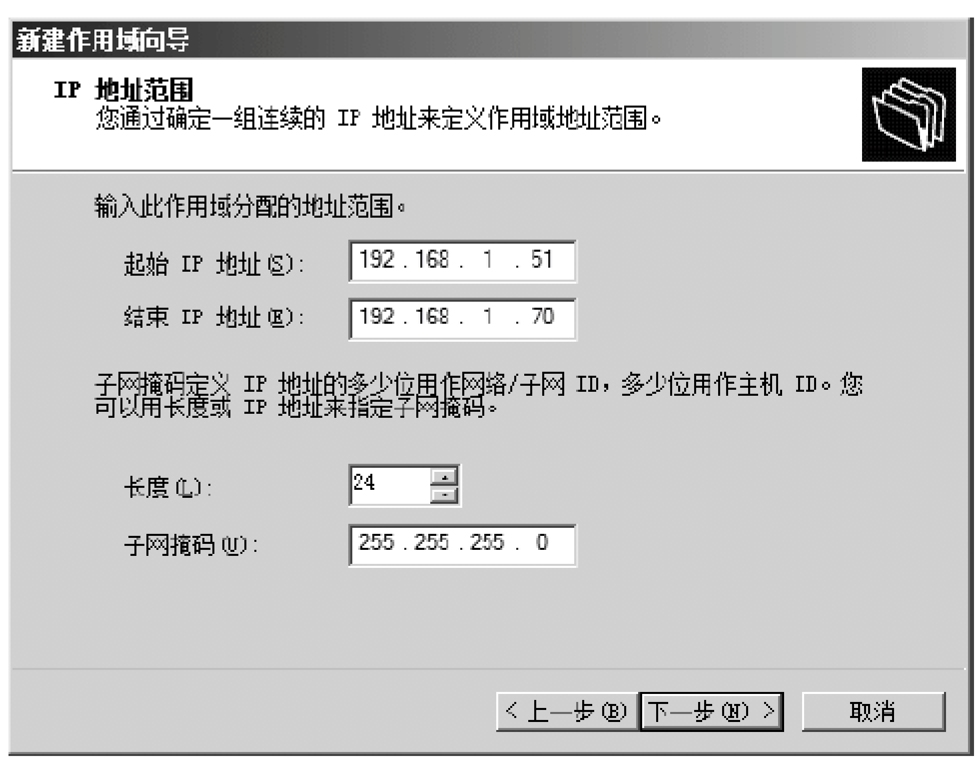


图 7-20　新建作用域向导-IP 地址范围

(4) 接下来是“添加排除”，如图 7-21 所示，管理员可以规定哪部分或是哪一个 IP 地址将被排除在自动分配的地址空间以外。

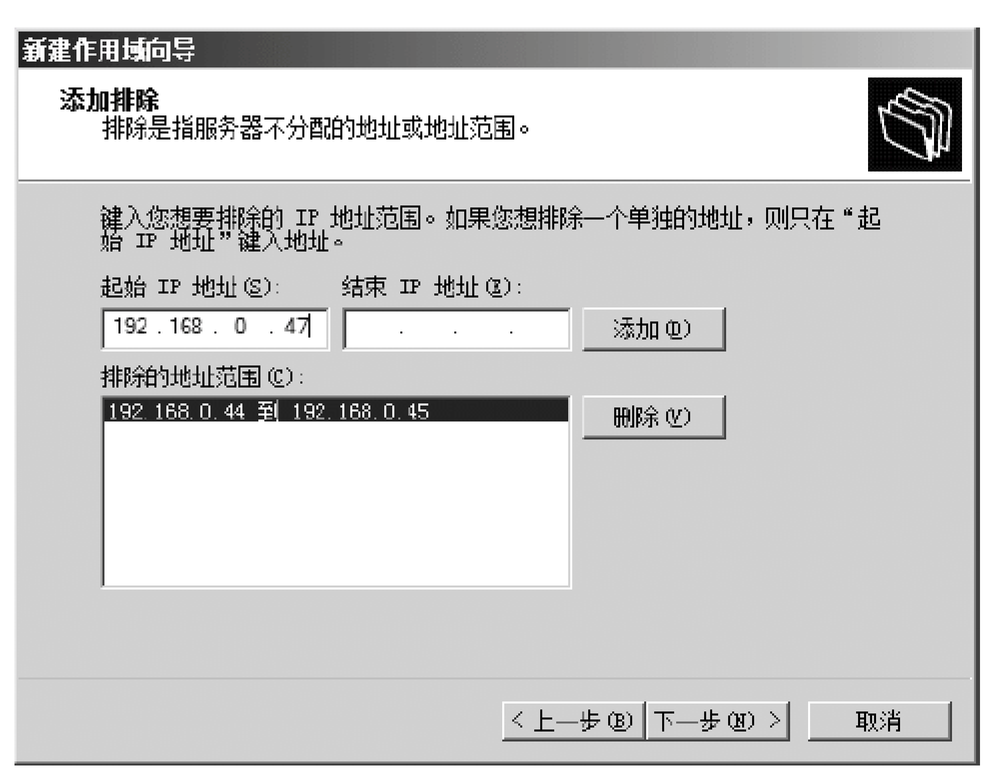


图 7-21　新建作用域向导-添加排除

(5) 第四步是设定作用域提供给 DHCP 客户端的 IP 地址的租用期限，如图 7-22 所示。对于主要包含台式计算机、结构相对固定的网络来说，租用期限可以设置得较长些；对于主要包含笔记本电脑或拨号客户端、结构灵活多变的网络来说，设置较短的租用期限更好些。

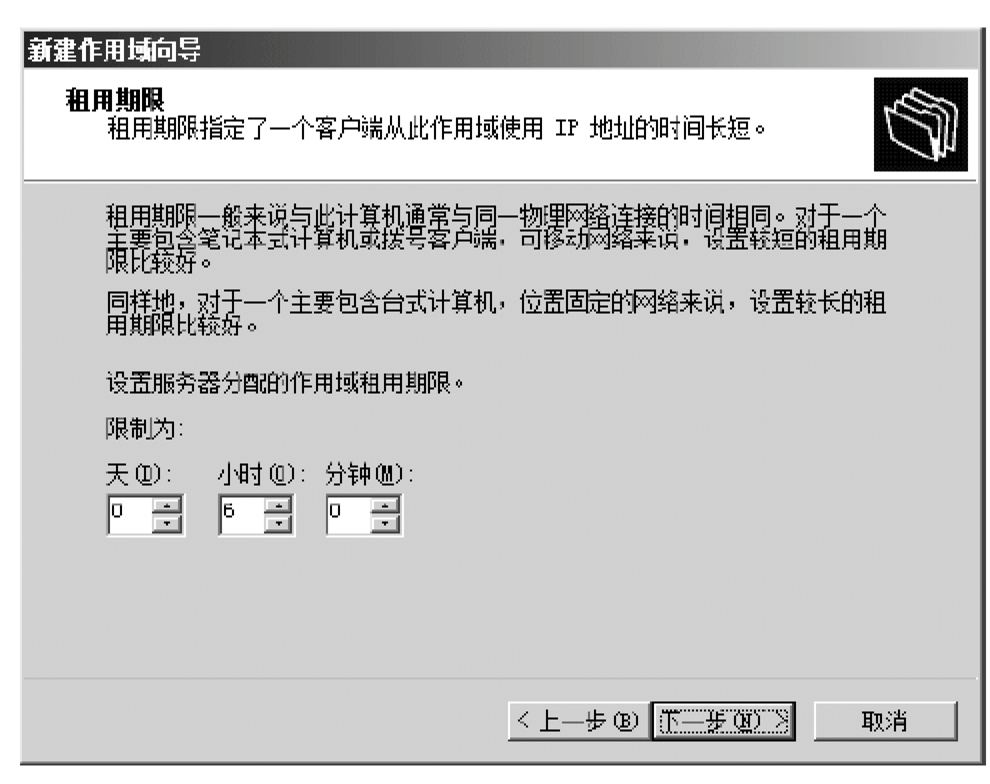


图 7-22　新建作用域向导-租用期限

(6) 接下来是配置 DHCP 选项，如图 7-23 所示。此处配置的 DHCP 选项为作用域选项。这些选项可以现在配置，也可以在建立作用域以后再另行配置。

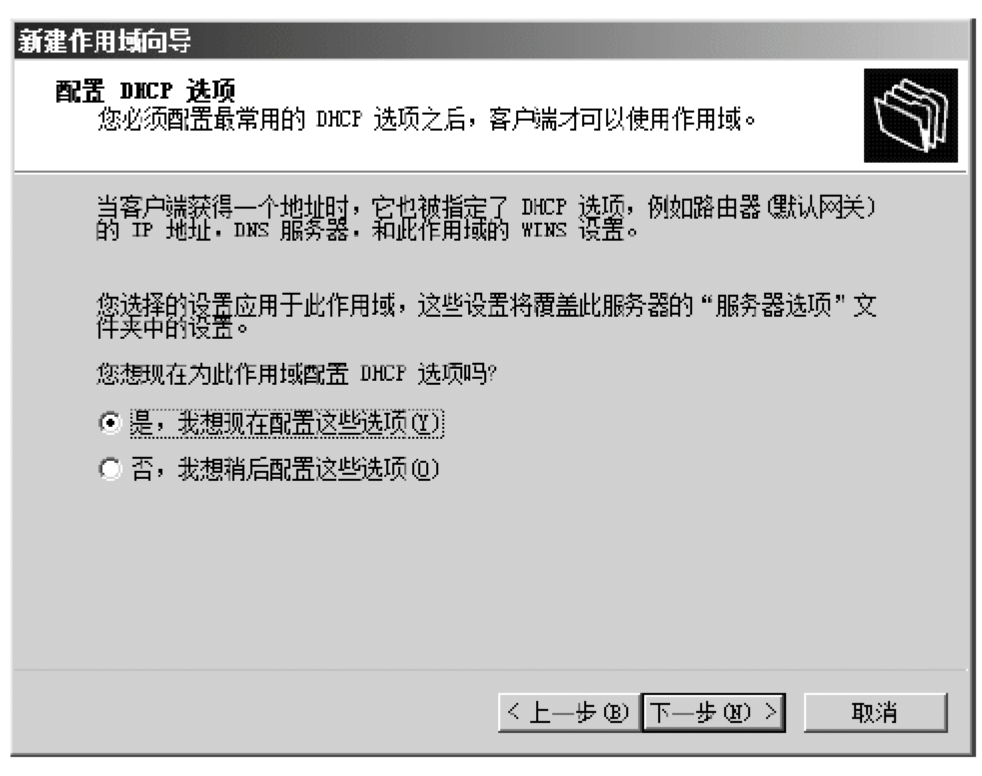


图 7-23 新建作用域向导-配置 DHCP 选项

(7) 如果在上一步骤中选择“是，我想现在配置这些选项”，则接下来的 3 个步骤中，向导会依次要求管理员输入路由器 IP 地址、域名称、DNS 服务器名称及 IP 地址和 WINS 服务器名称及 IP 地址等相关信息。

(8) 最后，向导询问是否马上激活新建的作用域，如图 7-24 所示，通常都应选择“是，我想现在激活此作用域”。然后单击“下一步”按钮，向导将会开始创建新的作用域，并在创建完毕后提示创建成功的信息，如图 7-25 所示。

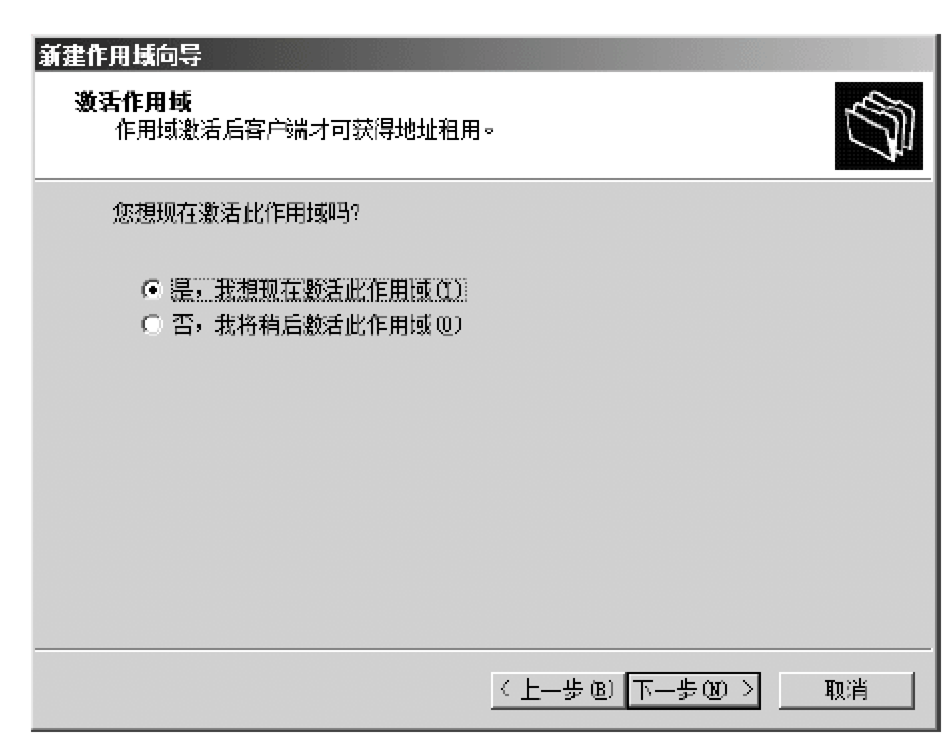


图 7-24 新建作用域向导-激活作用域

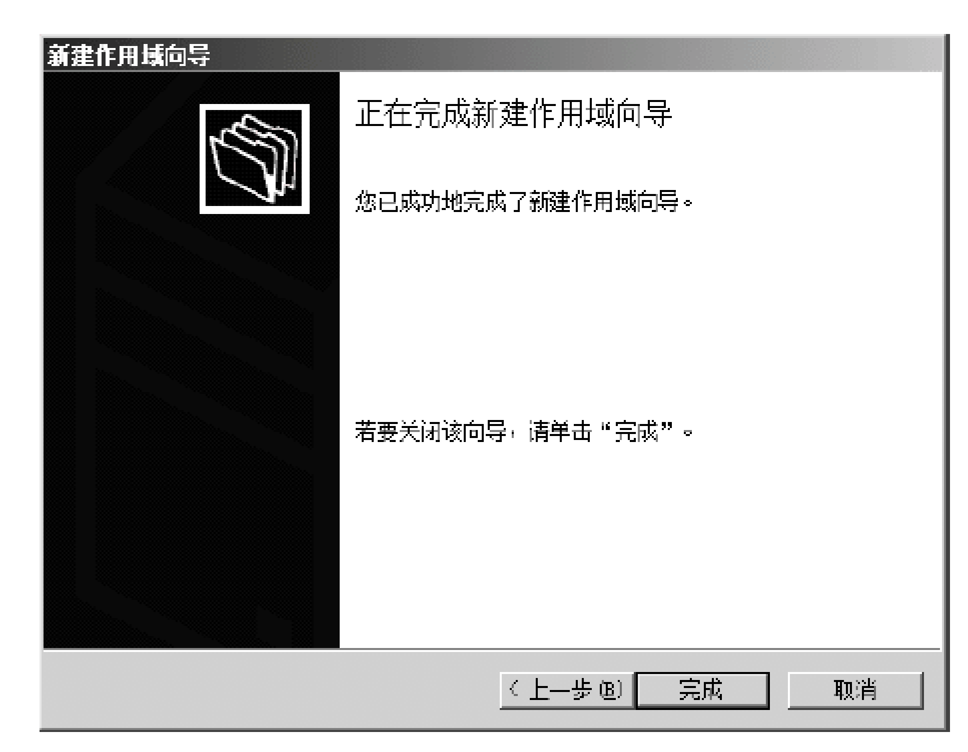


图 7-25 新建作用域向导-完成新建作用域向导

7.3.3 作用域的设置

在新建作用域的过程中设定相关的各个选项并激活以后，作用域就可以开始工作了。一般情况下不需要更改作用域的选项。但是当网络环境发生变化，或网络管理的要求改变的时候，也需要修改现有作用域的选项设置。

在 DHCP 控制台左侧的树状列表中选择相应的 DHCP 服务器，在服务器包含的对应的

作用域上右击，在弹出的快捷菜单中选择“属性”命令，即可弹出“作用域属性”对话框，如图 7-26 所示。在此对话框中就可以查看或修改作用域的各个选项设置了。

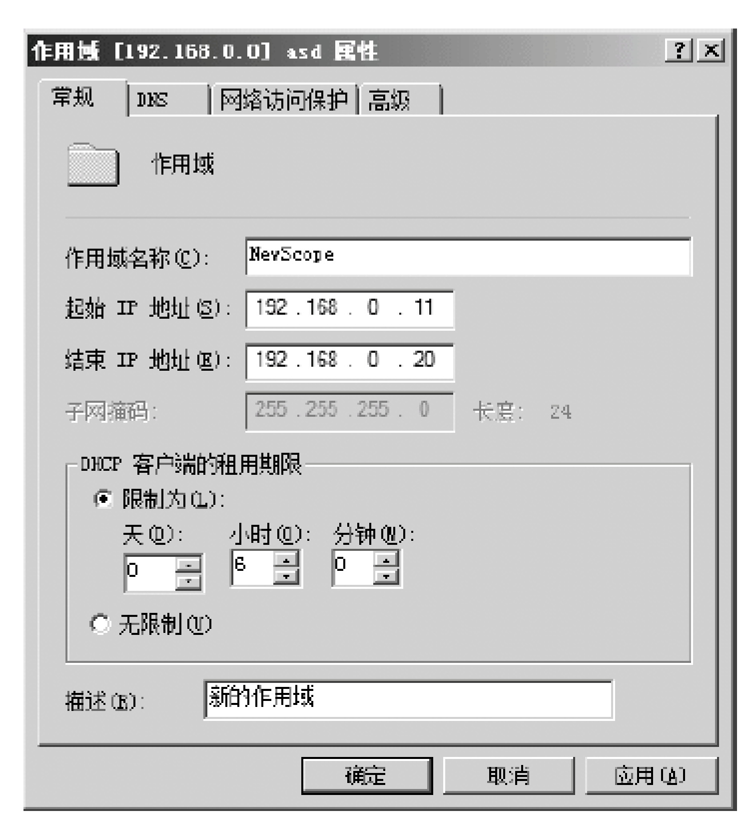


图 7-26　“作用域属性”对话框

7.3.4　保留 IP 地址

在网络中有时需要给某些特定的 DHCP 客户端如 FTP 服务器、打印服务器等分配固定的 IP 地址，这些固定的 IP 地址必须为特定的 DHCP 客户端保留下来，不能再分配给其他客户端，这可通过 DHCP 服务器的“保留”功能来实现。“保留”功能可以确保当特定的 DHCP 客户端向 DHCP 服务器请求获得 IP 地址或更新 IP 地址租约的时候，DHCP 服务器都会给该客户端分配其需要的同一个 IP 地址。

设置保留 IP 地址，只需在 DHCP 控制台中展开相应的作用域，在作用域的“保留”项上右击，在弹出的快捷菜单中选择“新建保留”命令，即可弹出“新建保留”对话框，如图 7-27 所示。此对话框中需要设置以下选项：



图 7-27　“新建保留”对话框

- 保留名称：设置保留项的名称，用于与其他保留项区分。
- IP 地址：即需要为特定 DHCP 客户端保留的 IP 地址。

- MAC 地址：此处应输入要保留 IP 地址的 DHCP 客户端网卡的 MAC 地址。这是 DHCP 服务器识别客户端的重要标志。只有使用该 MAC 地址的 DHCP 客户端网卡才能获得该保留地址。
- 描述：对使用保留地址的 DHCP 客户端做一个简单的描述。此项为可选项。
- 支持的类型：设置客户端所支持的 DHCP 服务类型。其中 BOOTP 是为兼容早期无盘工作站而设计的，普通的客户端计算机可选择“仅 DHCP”或“两者”。

设置相关参数后，单击“添加”按钮，即可建立特定 IP 地址与特定 DHCP 客户端之间的关系，保证将此 IP 地址保留给该 DHCP 客户端使用。重复操作，就可以添加多个保留 IP 地址。

7.3.5　超级作用域

当网络环境变得越来越复杂时，DHCP 客户端的种类、数量和要求也会越来越多，一台 DHCP 服务器上往往会有多个作用域，每个作用域用于管理网络中的一部分主机并独立地提供配置信息。多个作用域增大了网络管理员的管理复杂度，降低了管理效率，于是超级作用域应运而生。它可以将 DHCP 服务器上的多个作用域合并为一个超级作用域，把它作为单个实体来管理。如果在同一个物理网段上存在多个 DHCP 作用域，分别管理分离的逻辑 IP 网络结构，就可以通过使用超级作用域来组合并激活所有被包含的作用域，并通过这种方式为客户端提供来自多个作用域的租约。

超级作用域的建立也是通过 DHCP 控制台实现的。步骤如下：

(1) 在 DHCP 控制台中右击要创建超级作用域的 DHCP 服务器，在弹出的快捷菜单中选择“新建超级作用域”命令，即可弹出如图 7-28 所示的“新建超级作用域向导”对话框。

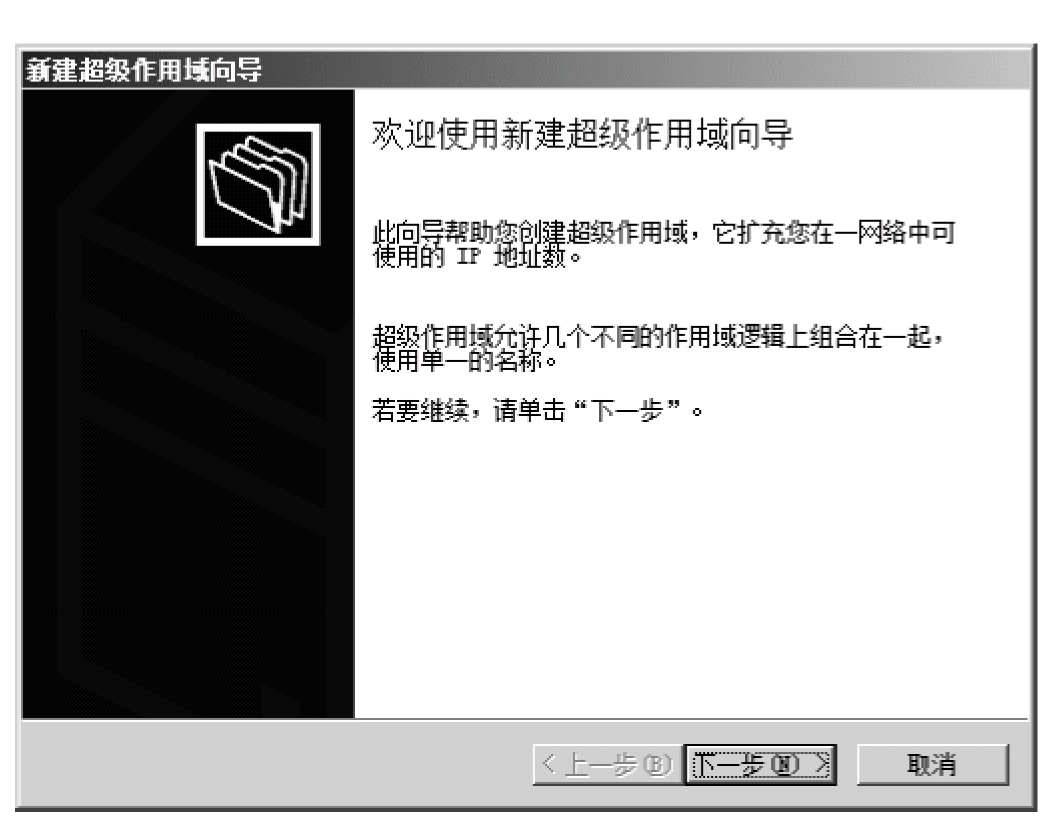


图 7-28　“新建超级作用域向导”对话框

(2) 单击“下一步”按钮，在“超级作用域名”步骤中给新建的超级作用域输入一个名称，如图 7-29 所示。



图 7-29　新建超级作用域向导-超级作用域名称

(3) 单击“下一步”按钮，在“选择作用域”步骤中会列出当前 DHCP 服务器中现有的可用作用域列表，如图 7-30 所示。在表中选择需要加入到超级作用域的一个或多个作用域，然后单击“下一步”按钮。

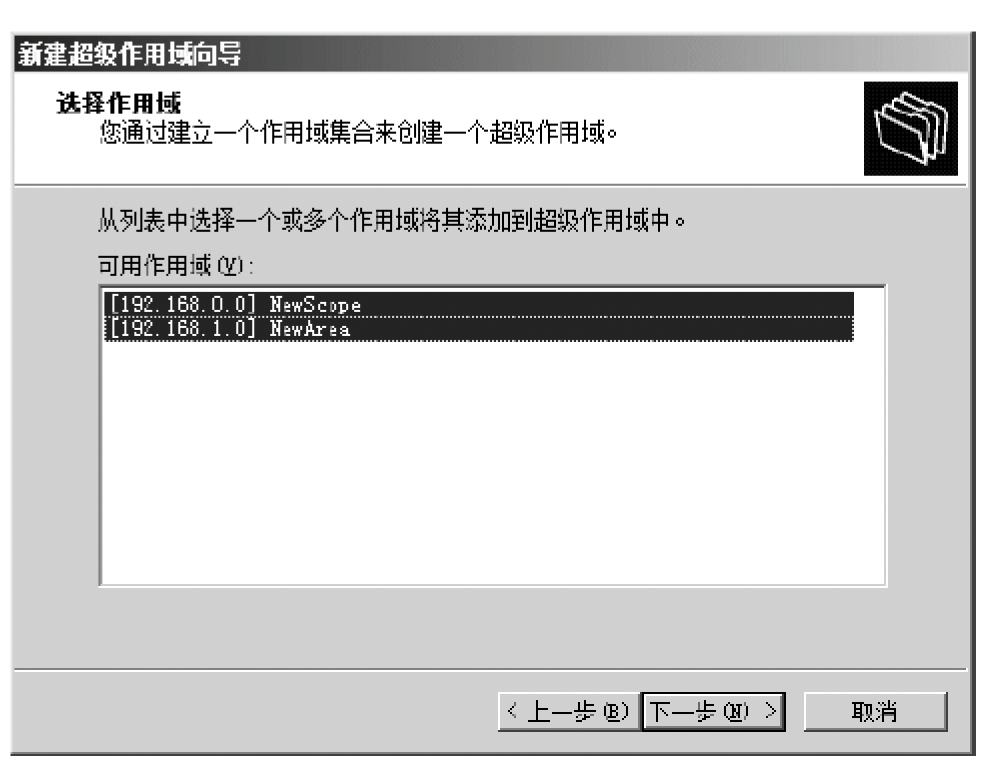


图 7-30　新建超级作用域向导-选择作用域

(4) 在如图 7-31 所示的“正在完成新建超级作用域向导”，管理员在此可以审查超级作用域的名称及其包含的作用域是否符合要求。

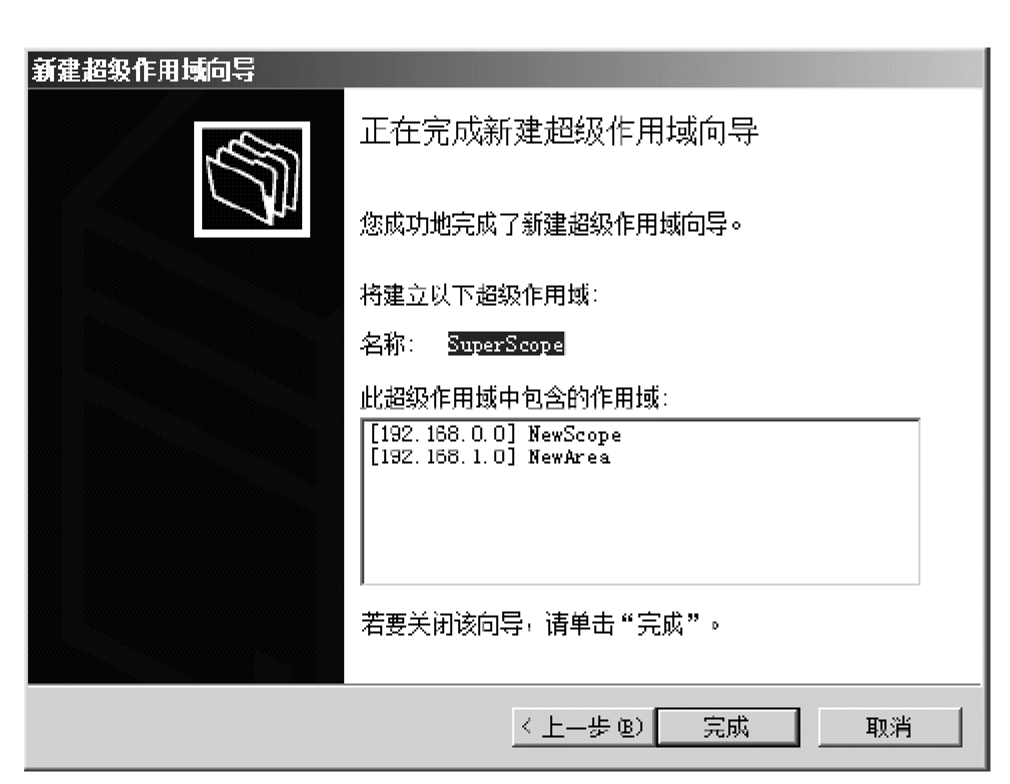


图 7-31　新建超级作用域向导-正在完成向导

(5) 单击“完成”按钮，超级作用域创建成功，并显示在 DHCP 控制台列表中，如图 7-32 所示。原有的作用域就像是超级作用域中的下一级目录，便于分类管理。

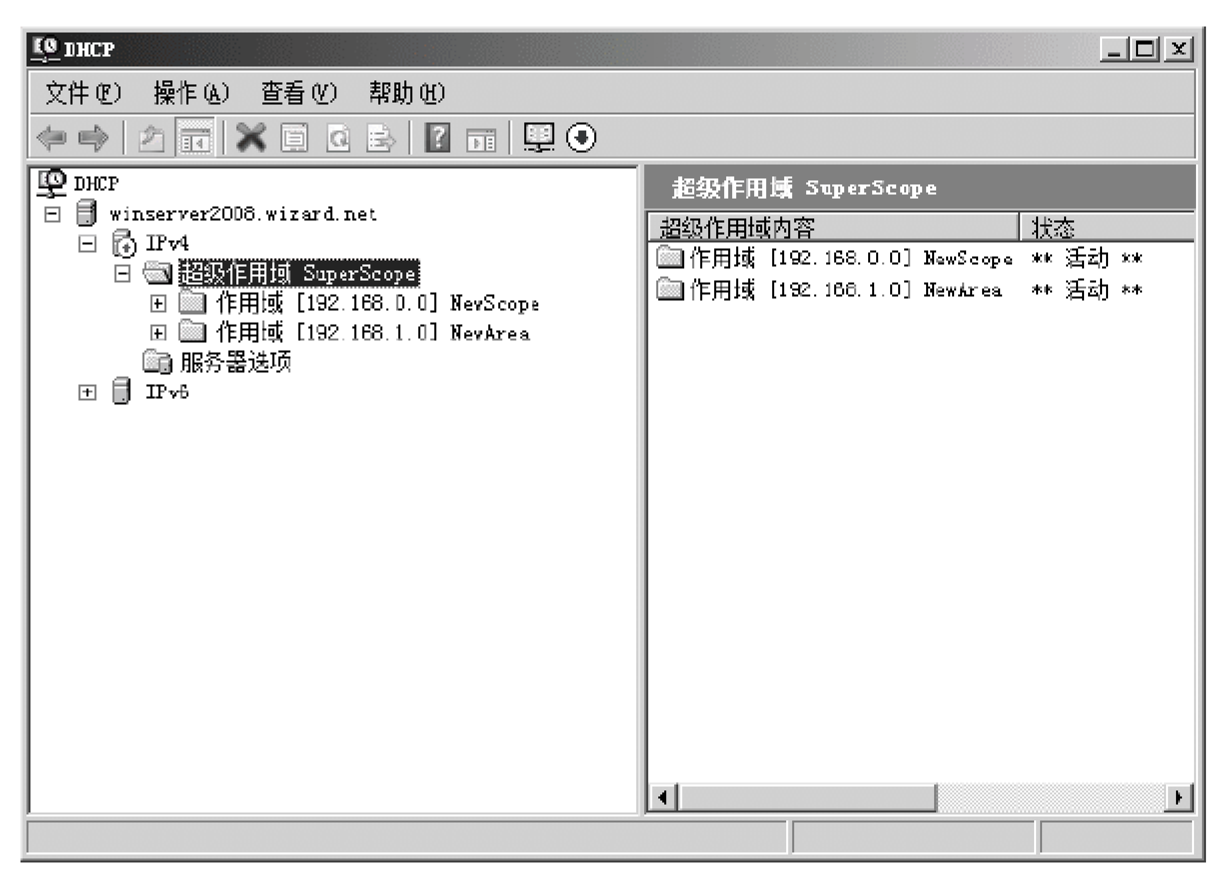


图 7-32　建立完成的超级作用域

创建超级作用域以后，还可以随时做进一步的调整，比如将某个作用域添加到超级作用域中，或者将某个作用域从超级作用域中删除，甚至在不需要超级作用域的时候将整个超级作用域删除。当然删除超级作用域并不会影响它所包含的作用域，因为超级作用域只是一个简单的容器，它里面所包含的作用域是不会被同时删除的。

7.4　DHCP 服务器的维护

DHCP 服务器的维护需求很小，只有在出现问题例如 DHCP 作用域的地址空间被耗尽或要将 DHCP 服务器迁移到别的计算机上时才需要维护。

7.4.1　数据库的备份与还原

DCHP 服务器的作用就是配置和管理网络中 DHCP 客户端的 IP 地址等相关信息，一旦服务器发生故障，不仅客户端计算机无法获取 IP 地址信息，原来的作用域及保留地址等相关设置也会丢失，从而影响网络的正常运行。因此，对 DHCP 服务器数据的备份显得尤为重要。

DHCP 服务器的数据都保存在%Systemroot%\system32\dhcp 文件夹里，其中 dhcp.mdb 作为存储数据库文件，其他文件为辅助文件，还有一个 backup 文件夹，用来存放备份 DHCP 数据库文件。DHCP 服务器默认情况下每小时会自动将 DHCP 数据库文件备份到该文件夹中。因此通过复制 backup 文件夹的所有内容可以达到备份 DHCP 服务器数据的目的。每次 DHCP 服务器启动的时候都会自动检查 DHCP 数据库是否损坏，如果发现损坏，就自动使用%Systemroot%\system32\dhcp\backup 文件夹中的备份数据进行数据还原。但是如果

backup 文件夹中的数据也被损坏，那么系统将无法完成自动还原工作，相关服务也无法正常启动。为了避免这一情况，在人工备份 DHCP 数据库的时候往往选择与 DHCP 服务器不同的计算机存储媒体进行备份。

由于 Windows Server 2008 对 DHCP 服务器的备份与还原做了优化，所以完全不需要直接对这些文件夹或文件进行操作，只需在 DHCP 控制台窗口中右击 DHCP 服务器的名称，在弹出的快捷菜单中选择“备份”命令，如图 7-33 所示，在弹出的“浏览文件夹”对话框中选择要保存备份文件的位置，如图 7-34 所示，然后单击“确定”按钮，即可完成备份操作。



图 7-33　备份 DHCP 数据库-选择备份

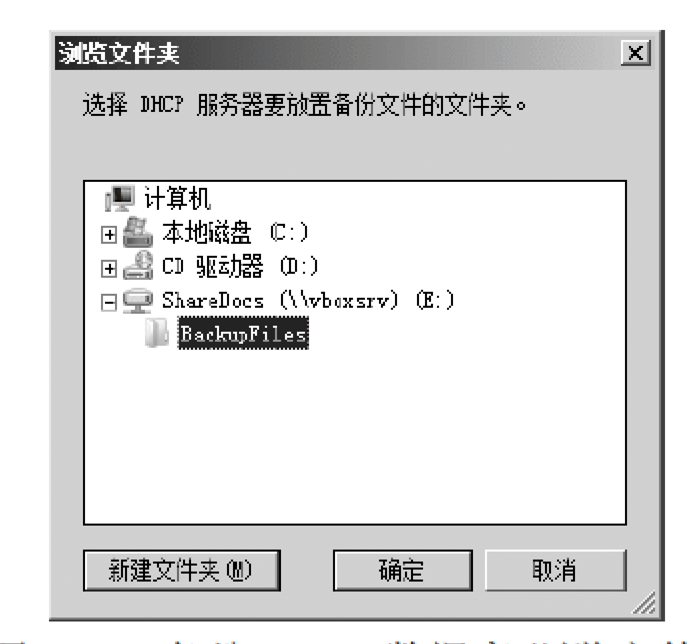


图 7-34　备份 DHCP 数据库-浏览文件夹

还原 DHCP 数据库的操作也同样简单，只需在 DHCP 控制台窗口中右击 DHCP 服务器的名称，在弹出的快捷菜单中选择“还原”命令，如图 7-35 所示，在弹出的“浏览文件夹”对话框中选择备份文件所在的位置，如图 7-36 所示，然后单击“确定”按钮，即可完成还原操作。



图 7-35　还原 DHCP 数据库-选择还原



图 7-36　还原 DHCP 数据库-浏览文件夹

需要注意的是，为了保持数据的一致性，无论备份还是还原 DHCP 数据库，都不能在 DHCP 服务运行的时候进行。备份 DHCP 数据库的时候，服务器会自动暂停 DHCP 服务，待备份完毕后再自动开启服务。还原 DHCP 数据库的时候，系统也会弹出如图 7-37 所示

的信息框，告诉管理员在还原 DHCP 数据库的时候系统会自动停止并重新启动 DHCP 服务。

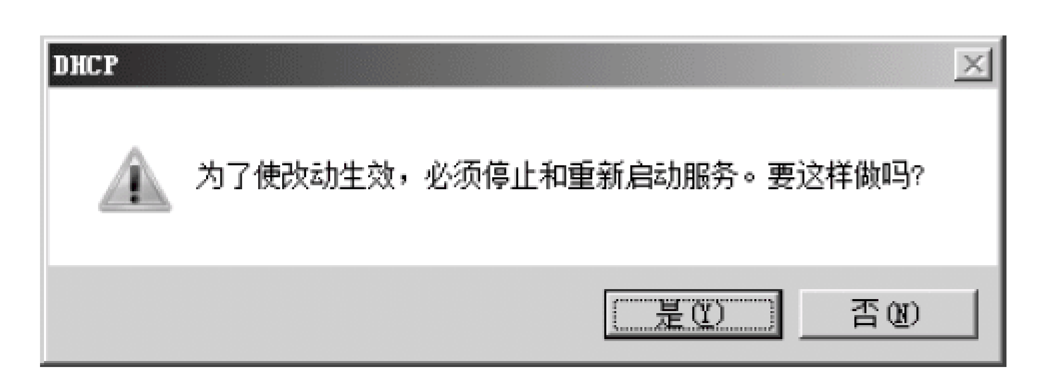


图 7-37　还原 DHCP 数据库-警告信息

7.4.2　服务器迁移

有时因为硬件配置的升级限制，或是服务器所在物理位置的变化，原有的 DHCP 服务器已不能满足要求，这就需要用一台新的 DHCP 服务器替代原有的服务器。而原有服务器上往往已经包含了关于作用域、保留地址以及大量 DHCP 选项的设置，如果在新 DHCP 服务器上全部进行重新设置，难免会因疏漏造成错误。通过对旧服务器上的 DHCP 数据库进行备份，然后转移到新服务器上进行还原来实现服务器的迁移，是一种简单而又不易出错的方法。

1. 旧 DHCP 服务器上的操作

步骤如下：

(1) 为确保数据的一致性，首先停止 DHCP 服务。

(2) 将%Systemroot%\system32\dhcp 文件夹中的所有文件及文件夹全部备份出来。

(3) 将注册表中键值为“HKEY_LOCAL-MACHINE \ SYSTEM \ CurrentControlSet \ Services \ DHCP Server”的注册表内容导出到一个注册表文件中。

2. 新 DHCP 服务器上的操作

步骤如下：

(1) 首先确保服务器上已经安装了 DHCP 服务器角色，且当前 DHCP 服务处于停止状态。

(2) 将旧 DHCP 服务器上备份出来的%Systemroot%\system32\dhcp 文件夹中的所有文件及文件夹复制到新 DHCP 服务器的相应位置。

(3) 将从旧 DHCP 服务器上导出的注册表文件导入到新 DHCP 服务器中注册表的相应键值的位置。

(4) 重新启动 DHCP 服务，然后在 DHCP 控制台中右击 DHCP 服务器名称，在弹出的快捷菜单中选择“协调所有作用域”命令，在弹出的“协调所有作用域”对话框中单击“验证”按钮，如图 7-38 所示，如果显示验证一致的信息，如图 7-39 所示，则表明迁移成功，新的 DHCP 服务器已经可以正常工作。

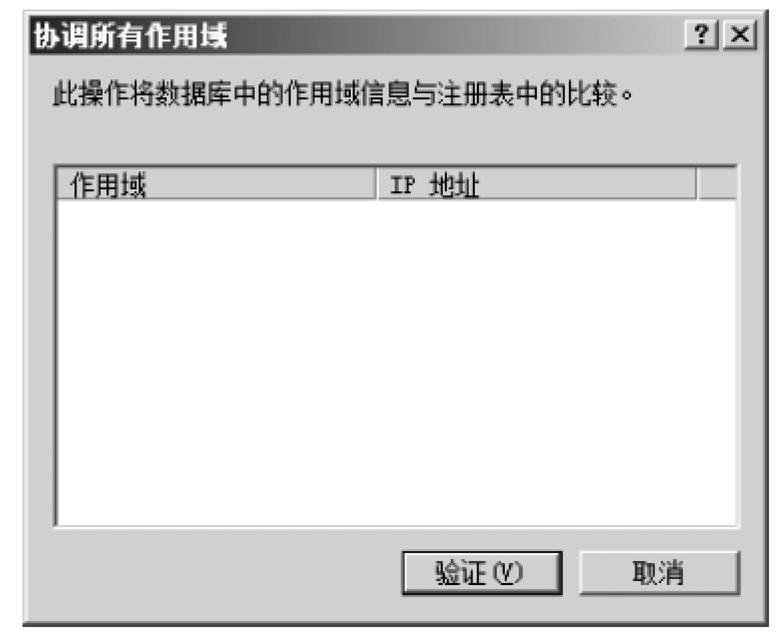



图 7-38　协调所有作用域对话框



图 7-39　DHCP 迁移-验证一致

需要注意的是，新 DHCP 服务器在网络连接上的设置如网络适配器的数量及网络适配器所连接的网络等应该与原有的 DHCP 服务器相一致或是相兼容的，否则就有可能导致服务器迁移后 DHCP 服务无法正常启动。

7.5　DHCP 客户端的配置

网络中的 DHCP 服务器一旦配置完成，就意味着绝大部分工作都做完了，DHCP 客户端计算机只需设置为“自动获取 IP 地址”即可自动从 DHCP 服务器获得 IP 地址信息，并实现网络通信。下面以两种最常用的操作系统 Windows XP 和 Windows 7 为例，说明 DHCP 客户端计算机的配置过程。

7.5.1　配置 Windows XP 客户端

配置 Windows XP 客户端的操作步骤如下：

(1) 通过右击任务栏通知区域的“本地连接”图标，在弹出的快捷菜单上选择“打开网络连接”命令(也可以其他方式打开网络连接窗口)。

(2) 在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单上选择“属性”命令，打开如图 7-40 所示的“本地连接属性”对话框。



图 7-40　WindowsXP 的“本地连接属性”对话框

(3) 在“本地连接属性”对话框中选择“Internet 协议(TCP/IP)”项目，然后单击“属性”按钮，打开如图 7-41 所示的“Internet 协议(TCP/IP)属性”对话框。



图 7-41　WindowsXP 的“Internet 协议(TCP/IP)属性”对话框

(4) 在“Internet 协议(TCP/IP)属性”对话框中选中“自动获取 IP 地址”和“自动获取 DNS 服务器地址”单选按钮，再单击“确定”按钮保存设置，即可完成 DHCP 客户端的配置。客户端计算机就会自动搜索网络中的 DHCP 服务器，并自动从 DHCP 服务器上获取 IP 地址信息。

7.5.2　配置 Windows 7 客户端

步骤如下：

(1) 通过右击任务栏通知区域的“网络-Internet 访问”图标，在弹出的快捷菜单上选择“打开网络和共享中心”命令(也可从控制面板等其他途径打开网络和共享中心)。

(2) 在“网络和共享中心”窗口中单击“本地连接”链接，在弹出的“本地连接状态”对话框中单击“属性”按钮，打开如图 7-42 所示的“本地连接属性”对话框。

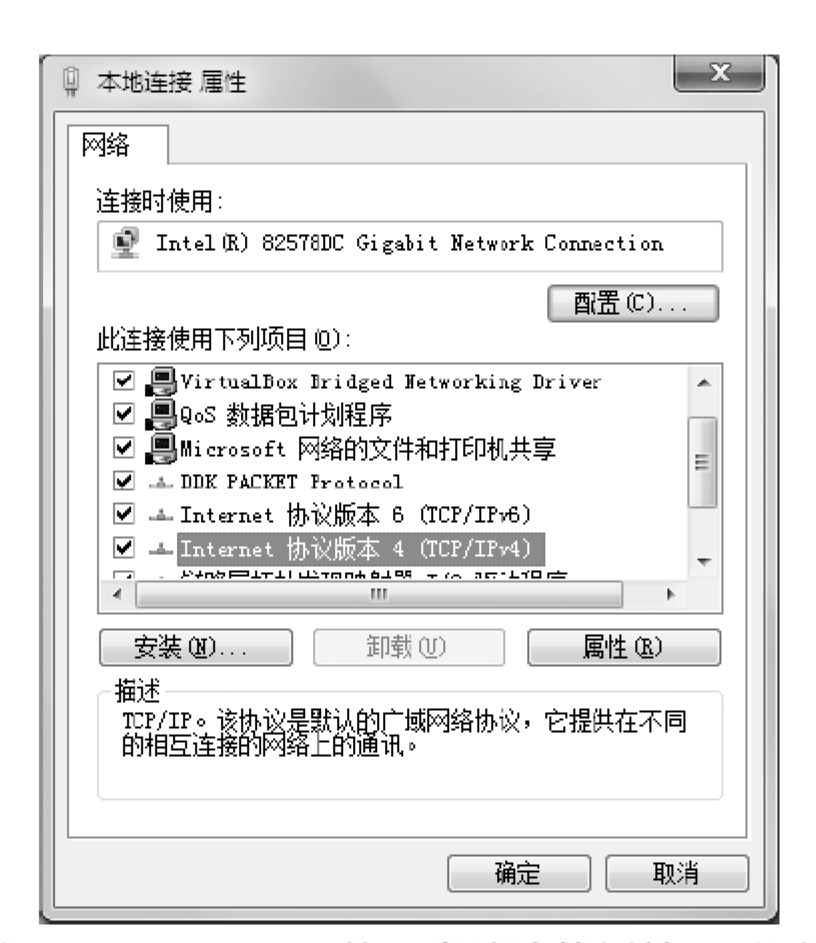


图 7-42　Windows7 的“本地连接属性”对话框

(3) 在“本地连接属性”对话框中选择“Internet 协议版本 4(TCP/IPv4)”项目，然后单击“属性”按钮，打开如图 7-43 所示的“Internet 协议版本 4(TCP/IPv4)属性”对话框。

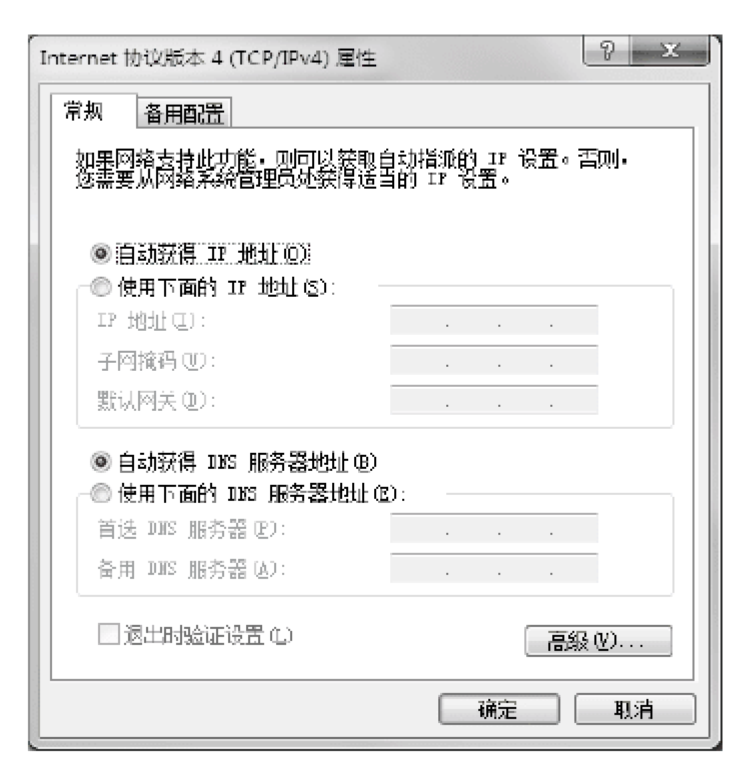


图 7-43　Windows7 的“Internet 协议版本 4(TCP/IPv4)属性”对话框

(4) 在“Internet 协议版本 4(TCP/IPv4)属性”对话框中选中“自动获得 IP 地址”和“自动获取 DNS 服务器地址”单选按钮，再单击“确定”按钮保存设置，即可完成 DHCP 客户端的配置。客户端计算机就会自动搜索网络中的 DHCP 服务器，并自动从 DHCP 服务器上获取 IP 地址信息。

7.6　本章小结

在 Windows Server 2008 系统中，可以通过“添加角色向导”来添加“DHCP 服务器”角色，从而在所属网络中部署 DHCP 服务器。当有 DHCP 客户端发出请求 DHCP 服务的广播信息后，DHCP 服务器就会响应请求，并从配置的地址范围内为客户端提供可用的 IP 地址。

安装好的 DHCP 服务器还必须经过授权才能开始工作，这是为了避免由于运行带有错误配置的 DHCP 服务器或者在错误的网络上运行配置正确的服务器而导致的大多数意外破坏。如果启动了未经授权的 DHCP 服务器，它可能开始为客户端租用不正确的 IP 地址或者否认尝试续订当前地址租约的 DHCP 客户端，这都会导致启用 DHCP 的客户端产生更多的问题。

DHCP 选项是 DHCP 服务器分配给客户端的配置设置如默认网关地址、DNS 服务器、WINS 节点类型等。管理员可以在添加“DHCP 服务器”角色时设置 DHCP 作用域和基本的 DHCP 选项，也可以通过“管理工具”中的 DHCP 控制台进行相关的 DHCP 选项设置。

7.7　思考与练习

【思考题】

1. DHCP 服务的全过程可分为哪几个阶段？

2. DHCP 服务器允许管理员从哪几个级别管理 DHCP 选项？不同级别的 DHCP 选项分别作用于什么范围？当不同级别的 DHCP 选项设置之间有冲突时，系统如何处理？

3. 建立作用域的过程中需要指定哪些参数设置？

4. 为什么要设置保留 IP 地址？如何设置保留 IP 地址？

【练习题】

初始条件：一台已安装并启用 DHCP 服务的 Windows Server 2008 服务器、服务器管理员帐户、已连通的本地网络、网络打印机；

操作目标：在已安装并启用 DHCP 服务的 Windows Server 2008 服务器上新建一个 DHCP 作用域，作用域所包含的地址范围应为 192.168.3.101~192.168.3.120 和 192.168.3.201~192.168.3.220；同时指定网络打印机(MAC 地址为 00-25-D3-3B-FD-01)的 IP 地址必须为 192.168.3.110。

第8章　Web服务

【本章导读】

Web 服务是网络上最常用的服务之一，它可以为用户以最直观的方式提供大量信息和资源，如信息查询、广告发布、商务活动以及社交活动等，Web 服务在网络中发挥着至关重要的作用。Windows Server 2008 中的 IIS 组件可以提供强大的 Web 服务，不仅支持静态网站发布信息，也可以支持 ASP、.Net 等动态网站技术来实现网站和用户的交互，使用户获得更好的使用体验。同时 IIS 简单、易用、便于管理，为客户节约了使用和维护成本。

8.1　Web 服务的搭建与配置

Windows Server 2008 通过 IIS(Internet 信息服务)提供 Web 服务。IIS 是一个综合性的服务组件，可以提供 WWW、FTP、SMTP 等服务，并可以对这些服务进行统一的管理。

如果要在 Windows Server 2008 上安装 IIS，至少应该做好以下几项准备工作：

(1) 安装 IIS 的 Windows Server 2008 服务器最好拥有一个固定 IP；

(2) 如果提供的 Web 服务是面向 Internet 的，那么这个网站最好拥有一个域名；

(3) 这个网站的域名和 IP 地址应该被加入 DNS 服务器；

(4) Web 网页最好保存在 NTFS 文件系统的分区中，以加强安全性。

8.1.1　Web 服务器的安装

在默认状态下，Windows Server 2008 是没有安装任何服务的，因此需要手动添加相应的服务。Windows Server 2008 中提供 Web 服务的组件是 Internet 信息服务，即 Internet Information Services，简称 IIS。安装方法如下：

(1) 依次选择“开始”→“管理工具”→“服务器管理器”，打开服务器管理器，在左侧窗口选择“角色”，在右侧窗口单击“添加角色”，打开添加角色向导，如图 8-1 所示。



图 8-1　“选择服务器角色”界面

(2) 选择“Web 服务器(IIS)”，此时会弹出对话框询问是否添加必须的 Windows 进程激活服务，如图 8-2 所示。



图 8-2　添加功能

(3) 单击“添加必需的功能”按钮，返回到添加角色向导，然后单击“下一步”按钮，进入“Web 服务器(IIS)”界面，再单击“下一步”按钮，进入“选择角色服务”界面，如图 8-3 所示。

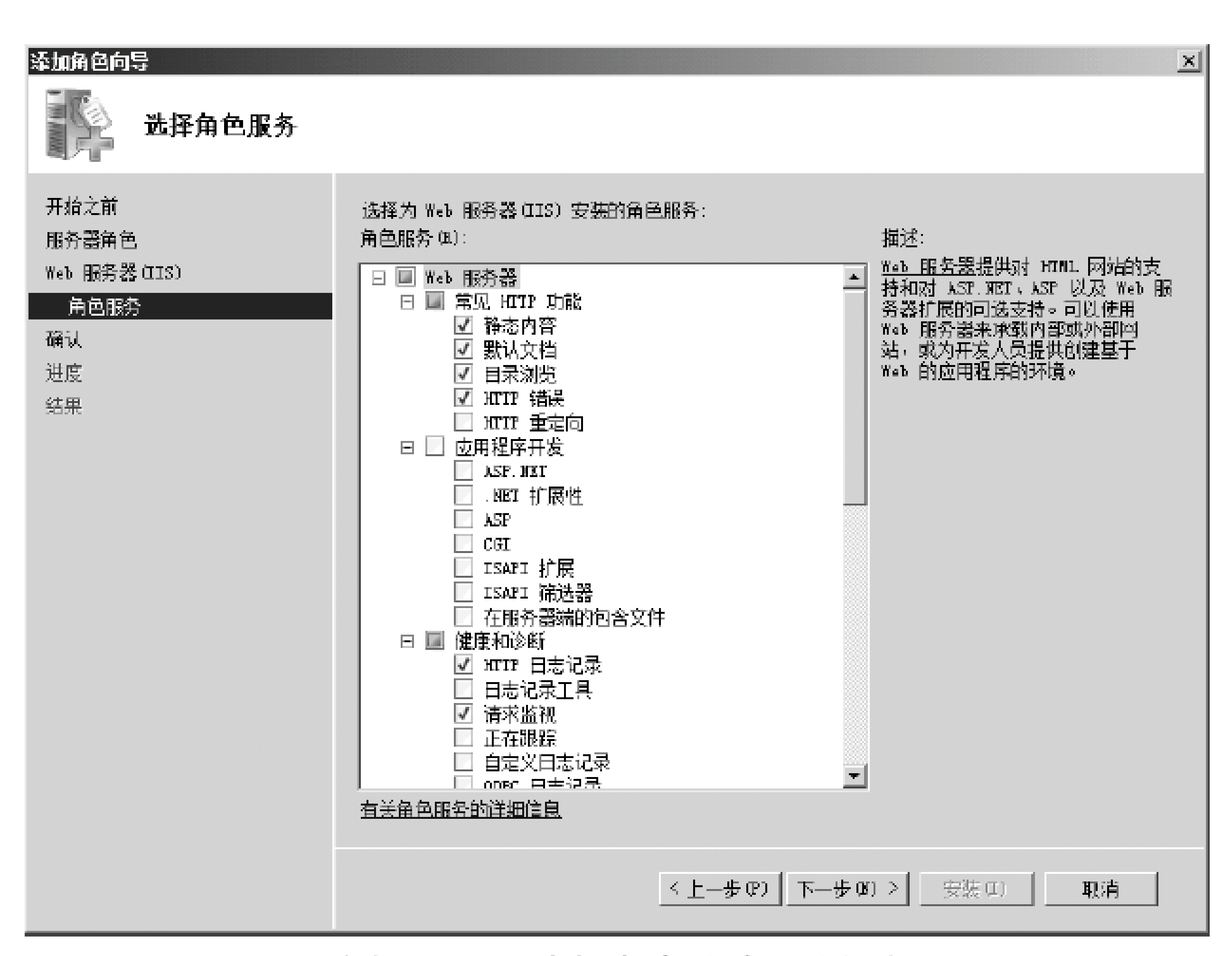


图 8-3　“选择角色服务”界面

(4) 如果网站需要使用 ASP.NET 技术，则选中“应用程序开发”中的子项 ASP.NET 和 ASP，此时会弹出对话框询问是否要添加必须的角色和功能，如图 8-4 所示。

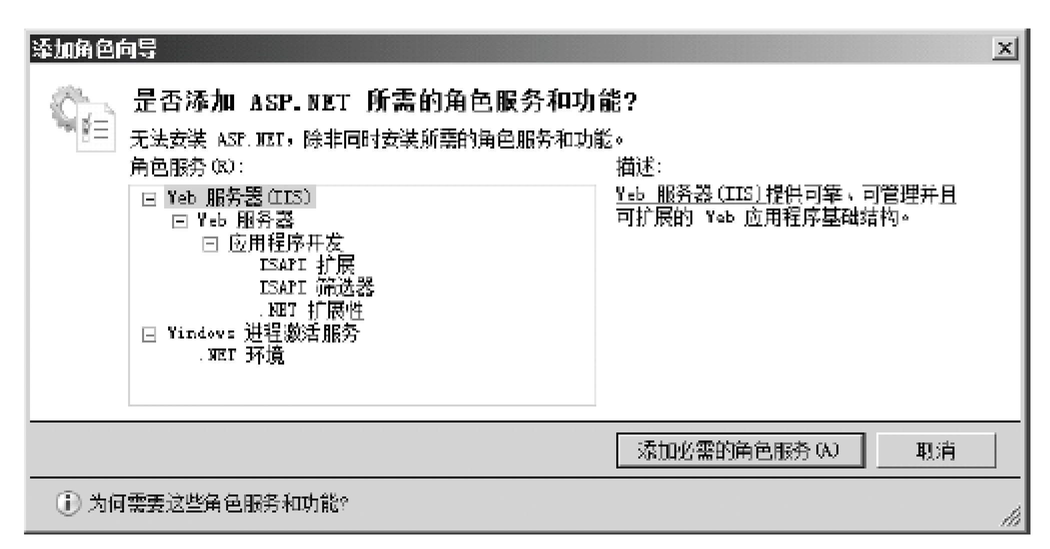


图 8-4　添加功能

(5) 单击“添加必需的角色服务”，返回到向导中，单击“下一步”按钮，进入“确认安装选择”界面，如图 8-5 所示。



图 8-5　“确认安装选择”界面

(6) 单击“安装”按钮，等待几分钟后安装完毕，进入“结果”界面，单击“关闭”按钮即可完成安装。

(7) 依次选择“开始”→“管理工具”→“Internet 信息服务管理器”，打开“Internet 信息服务(IIS)管理器”，如图 8-6 所示。



图 8-6　“Internet 信息服务(IIS)管理器”界面

(8) 选择“连接任务”→“连接至 localhost”命令，能看到如图 8-7 所示的界面，说明 IIS 已安装成功。



图 8-7　“管理服务器”界面

(9) 或者打开 IE 浏览器，在地址栏中输入 localhost 或者 127.0.0.1，可以看到如图 8-8 所示的界面，也说明 IIS 已安装成功。



图 8-8　测试网站页面

8.1.2　Web 网站的基本配置

对于 Web 网站的基本配置包括以下几项。

1. 启动、停止和重启

在 IIS 中选中要配置的网站，右侧窗口中有“重新启动”、“启动”和“停止”3 个

选项，分别可以使该网站重启、启动和停止。

当网站被停止时，用户是无法访问网站的，只有启动之后才能再次访问。

如果网站出现一些比较小的故障，或者进行某些设置，可以使用重启功能尝试恢复正常运行或使设置生效。

2. 设置主目录

IIS 安装完毕后，已经可以打开默认网站，管理员也可以将网站文件替换默认网站文件，或者将默认网站的主目录设置为自己的网站目录。

主目录就是网站文件所在的根目录，用于保存网站所有的网页、图片和声音等文件，默认路径为“C:\inetpub\wwwroot”，管理员可以将网站文件复制到该路径下。但是数据文件和操作系统文件在同一个卷中，一方面如果系统出现问题，需要重新安装系统时数据也会被破坏；另一方面如果系统被攻击，黑客一般会首先攻击默认设置的一些文件路径。修改主目录的具体操作方法如下：

(1) 打开 IIS 管理器，选择欲设置主目录的站点，在右侧窗口的“操作”栏中单击“基本设置”，打开“编辑网站”对话框，如图 8-9 所示。



图 8-9　“编辑网站”对话框

(2) 在“物理路径”对话框中输入网站主目录的路径，或者单击“浏览”按钮，在弹出的对话框中选择路径，然后单击“确定”按钮完成主目录的设置。

3. 地址绑定

一个网站建立完毕后，一般是通过 IP 地址或域名进行访问的，而且有些服务器网卡是可以拥有多个 IP 地址的，为了使网站能够被正确访问，应当正确设置网站的 IP 地址或域名。设置一个网站的地址或域名的具体操作方法如下：

打开 IIS 管理器，选择欲设置主目录的站点，在右侧窗口的“操作”栏中单击“绑定”，打开“网站绑定”对话框，如图 8-10 所示。



图 8-10　“网站绑定”对话框

选中目前已有的绑定设置，单击“编辑”按钮，打开“编辑网站绑定”对话框，如图 8-11 所示。

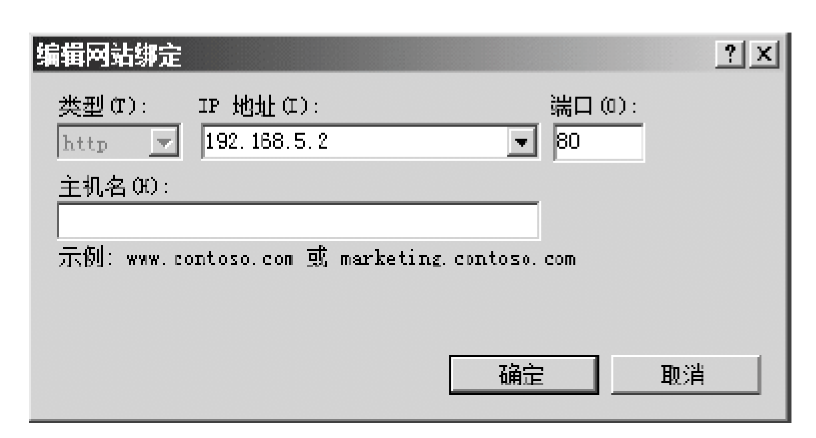


图 8-11　“编辑网站绑定”对话框

在“IP 地址”文本框中输入访问该网站时使用的 IP 地址，“端口”部分不用修改，保留默认的 80 端口。如果该网站拥有域名，可以将域名输入“主机名”文本框中，但是前提是该域名和 IP 已经被注册至 DNS 服务器。填写完毕后，单击“确定”按钮完成配置。

4. 默认文档

用户在访问网站时，一般只需要在浏览器中输入该网站的 IP 地址或域名，就可以打开网站的首页。那么服务器怎么知道哪个网页才是默认网页呢？Web 服务器均有定义默认文档的功能，默认文档就是当用户访问时，如果没有指明要访问的网页名，仅仅使用了 IP 地址或者域名，那么服务器将发送一个指定网页给用户，这个指定的网页就是默认文档。IIS 中设置默认文档的方法如下：

(1) 打开 IIS 管理器，选择要配置的网站名，在中间窗口找到“默认文档”图标，如图 8-12 所示。



图 8-12　IIS 管理器界面

(2) 双击“默认文档”图标，打开“默认文档”列表，如图 8-13 所示。目前该网站中有 6 个默认文档，分别是 Default.htm、Default.asp、index.htm、index.html、iisstart.htm 和 default.aspx。



图 8-13　“默认文档”设置界面

(3) 如果默认文档数目超过一个，则按照自上而下的顺序依次查找。如某网站的首页名为 index.htm，当用户向服务器发送请求后，服务器首先查找网站根目录下是否有名为 Default.htm 的网页文件，如果没有则查找名为 Default.asp 的网页文件，仍然没有找到的话继续查找名为 index.htm 的网页文件，此时查找成功，则停止查找，将该文件发送给用户，即使网站根目录中有名为 default.aspx 的网页文件也不会将其发送给用户。当一个默认文档名被选中，右侧窗口中出现了“操作”栏，管理员可以单击“上移”或“下移”选项以改变多个默认文档名之间的顺序，也可以单击“删除”按钮，删除选中的默认文档名。如果设计网站时使用的首页名不是当前默认文档名中的一个，可以单击“添加”选项，打开“添加默认文档”对话框，如图 8-14 所示。



图 8-14　“添加默认文档”对话框

(4) 在“名称”文本框中输入需要添加的默认文档名，然后单击“确定”按钮即可完成设置。

8.2　Web 服务器的管理

8.2.1　Web 网站的访问安全

IIS 中的 Web 网站默认情况下是允许匿名访问的，如果是 Internet 上的网站，必须允

许匿名访问，否则会造成很多不必要的麻烦。但在其他网络中，如大型企业中，往往各部门有自己的网站，其他部门的职员是不能访问的，此时需要禁用匿名访问，限制用户的访问。限制访问可以从访问限制、地址限制两个方面入手进行基本安全设置。

访问设置的操作方法如下：

(1) 在 IIS 管理器中选中欲设置的 Web 站点，如图 8-15 所示。



图 8-15　IIS 管理器界面

(2) 双击“身份验证”图标，打开“身份验证”设置界面，如图 8-16 所示。



图 8-16　“身份验证”设置界面

(3) 目前该 Web 站点允许匿名访问，在“匿名身份验证”上右击，在弹出的快捷菜单中选择“禁用”命令，匿名访问被禁止。

(4) 禁止匿名访问后，就可以设置身份验证了。IIS 中提供的身份验证有 3 种，分别是基本验证、Windows 身份验证和摘要身份验证。Windows Server 2008 中在默认状态下没有安装身份验证工具，需要手工添加。在“服务器管理器”中展开“角色”节点，选择“Web 服务器(IIS)”，单击“添加角色服务”，打开“选择角色服务”界面，如图 8-17 所示。

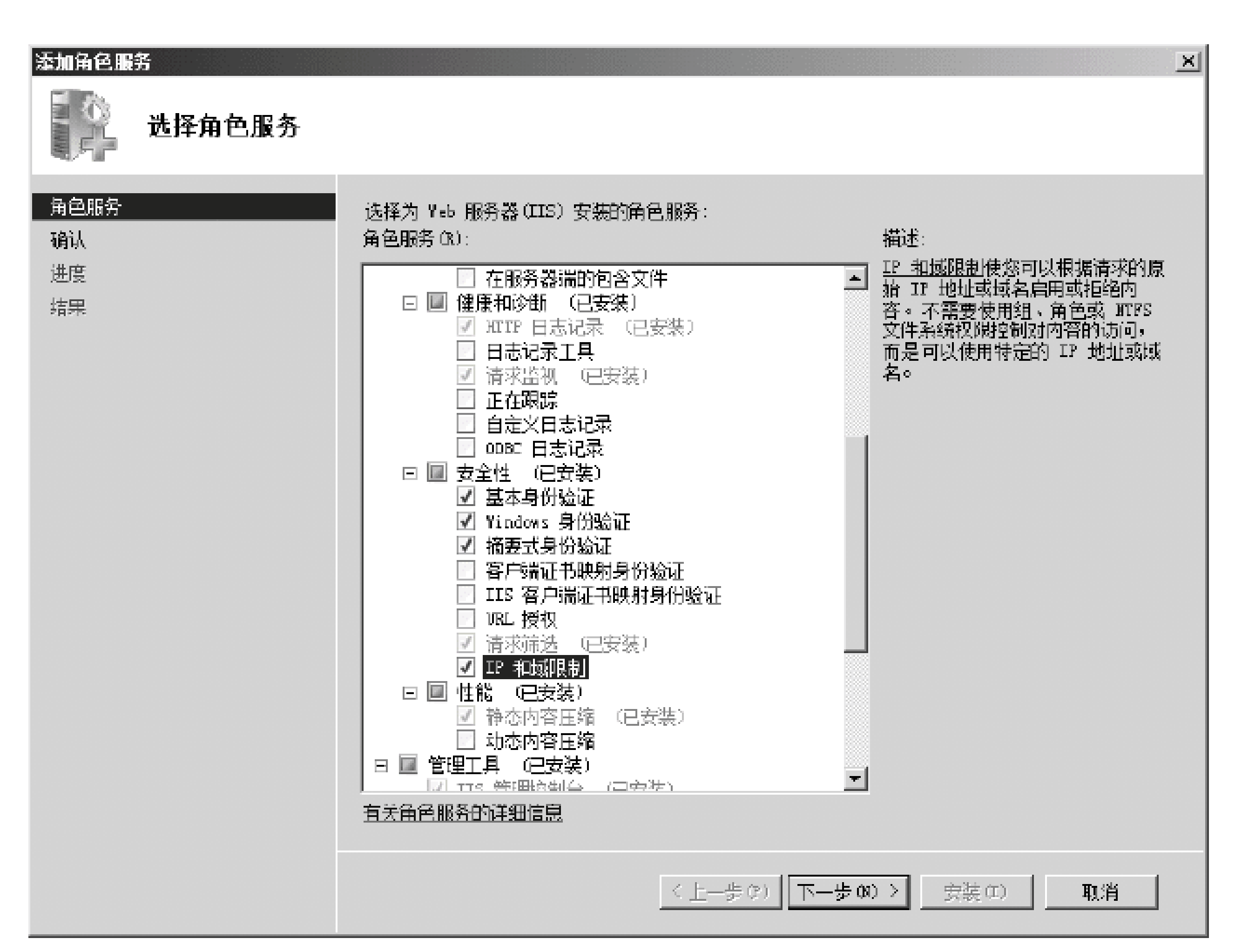


图 8-17　“选择角色服务”界面

(5) 在“安全性”选项中选择“基本身份验证”、“Windows 身份验证”、“摘要式身份验证”3 项，此外还可以选中“IP 和域限制”，以进行使用 IP 地址的限制。然后单击“下一步”按钮，根据向导提示，即可完成安装。3 种身份验证的含义分别如下。

- 基本身份验证：这种验证方法会使登录用户“模仿”为一个本地用户访问服务器，用于基本身份验证的 Windows 用户必须具有“本地登录”的用户权限。“基本身份验证”与浏览器良好兼容。这种身份验证方法适合于小型内部网络，在公共 Internet 上很少使用。基本身份验证的主要缺点是：它使用可被轻易解密的算法在网络上传输密码。如果这些密码被截获，破译它们将十分容易。建议将 SSL 与基本身份验证一起使用。
- Windows 身份验证：对于内部网站，Windows 身份验证是一种低成本的身份验证解决方案，同时用户使用时只需使用正确的用户名和密码登录自己的计算机即可，其他操作对于用户来说是透明的，降低了使用难度。这种身份验证方案允许 Windows 域中的管理员利用域基础结构来对用户进行身份验证，而且登录时的用户名和密码是经过加密处理才发送到服务器的，因此安全性更高。如果必须对其进行身份验证的用户从防火墙和代理服务器后访问网站，则不能使用 Windows 身份验证。
- 摘要式身份验证：使用摘要式身份验证方式时，会将密码哈希发送到 Windows 域控制器以对用户进行身份验证。当需要比基本身份验证更高的安全性时，可以考虑考虑使用摘要式身份验证。如果必须对其进行身份验证的用户从防火墙和代理服务器后访问网站，摘要是一种比 Windows 身份验证更好的身份验证方式。

(6) 安装完毕后，打开 IIS 管理器，打开要进行设置的网站的身份验证界面，对于需要的验证方式启动，不需要的禁用即可，如图 8-18 所示。



图 8-18　“身份验证”设置界面

(7) 打开 IIS 管理器，选中要进行设置的网站，双击窗口中间的“IPV4 地址和域限制”，打开“IPV4 地址和域限制”界面，如图 8-19 所示。

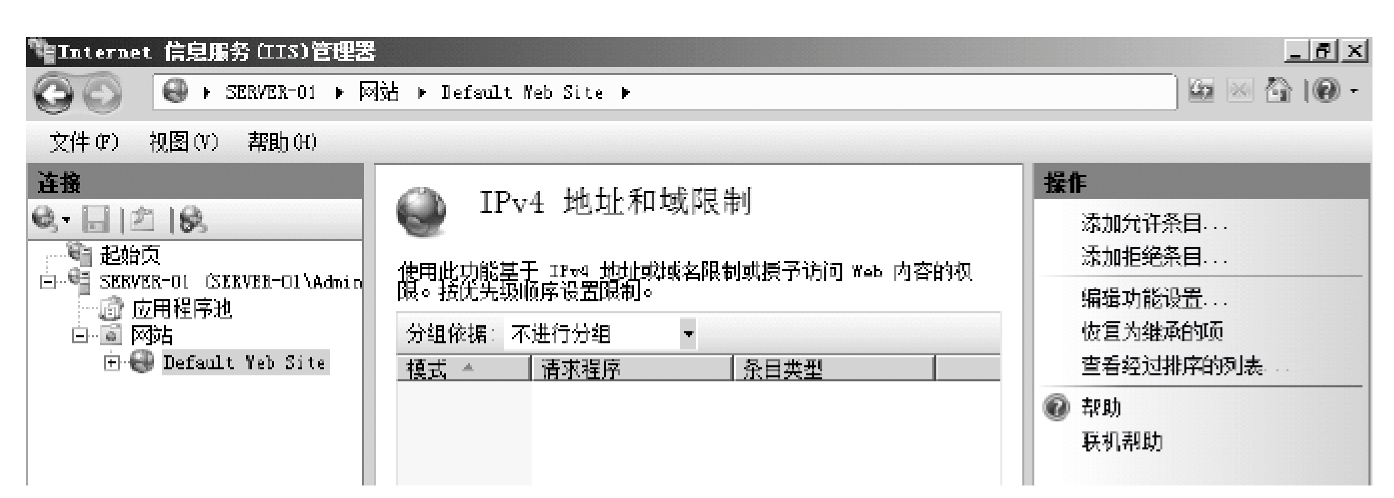


图 8-19　“IPV4 地址和域限制”界面

(8) 单击“添加允许条目”，打开“添加允许限制规则”对话框，如图 8-20 所示。

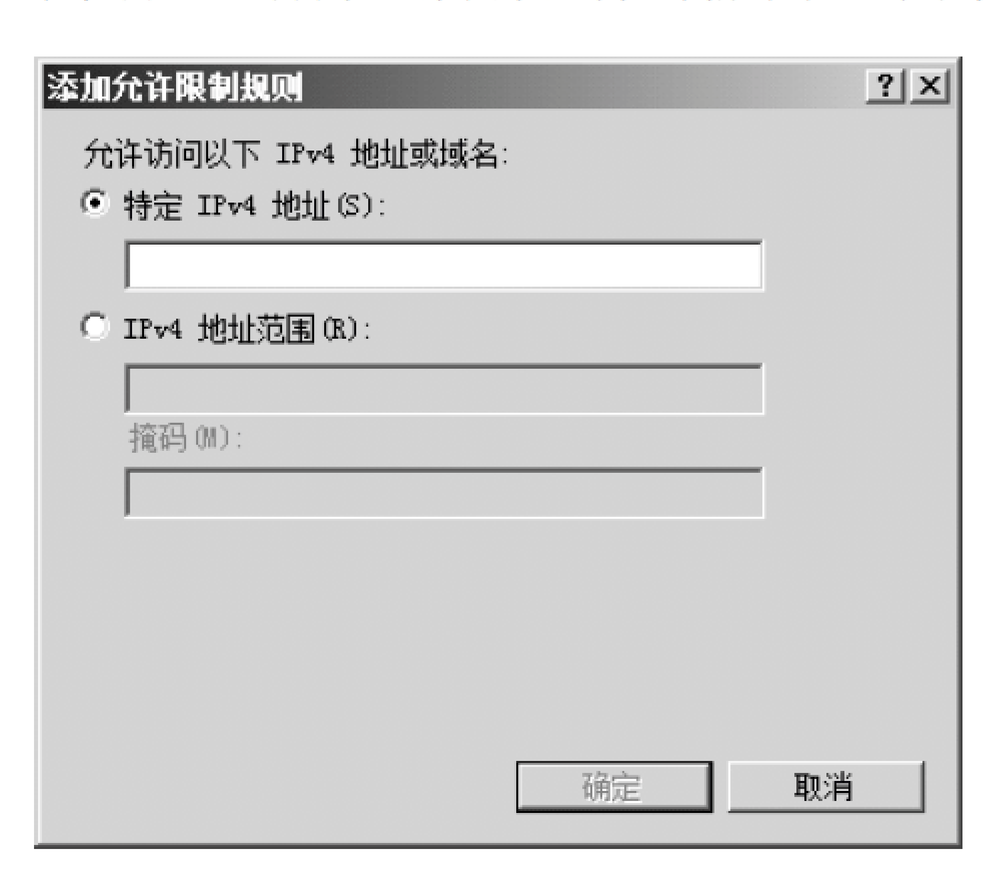


图 8-20　“添加允许限制规则”对话框

(9) 如果允许特定 IP 访问网站，则在“特定 IPv4 地址”文本框中输入指定 IP；如果允许一个 IP 地址段访问网站，则在“IPv4 地址范围”文本框中输入 IP 地址和子网掩码即可。输入完毕后，单击“确认”按钮以添加规则，可以添加多条规则。

(10) 如果不允许某个或某些 IP 地址访问网站，可以单击“添加拒绝条目”，在打开的“添加拒绝限制规则”对话框中输入 IP 地址或 IP 地址段，操作方法和添加允许访问的 IP

的方法相同，这里不再赘述。

8.2.2　虚拟目录的配置

虚拟目录并不是说该目录是虚拟的，而是指其目录名是虚拟的，目录本身仍然存在。在访问网站时，有时会看到这样的网址：http://sports.sohu.com/20110811/n316044615.shtml，在这个网址中，20110811 就是一个目录的名称，该网址表示现在访问的是网站 sports.sohu.com 中 20110811 目录下的 n316044615.shtml 网页。但是 20110811 仅仅是用户看到的目录名称，不一定是真实的目录名称，这就是虚拟目录。虚拟目录的作用是通过虚拟路径将存储在不同位置的文件和文件夹纳入到同一个网站下进行访问和管理。如一个网站的网址为 www.abcd.com，这个网站包含两个文件夹，即存储于 D 盘的文件夹 A 和存储于 E 盘的文件夹 B，那么可以通过虚拟目录，用户在访问网站时，可以通过 www.abcd.com/A 和 www.abcd.com/B 来访问两个文件夹下的网页，而不需要知道它们的具体路径。同时虚拟目录可以避免黑客通过访问网页而推测出网站中网页文件的存储结构，可以增加安全性。

虚拟目录可以在任何一个网站(包括虚拟网站)中创建，每个网站也可以创建多个虚拟目录。

创建和管理虚拟目录的方法如下：

(1) 打开 IIS 管理，在要添加虚拟目录的网站上右击，如图 8-21 所示。



图 8-21　IIS 管理器界面

(2) 选择快捷菜单中的“添加虚拟目录”命令，打开“添加虚拟目录”对话框，如图 8-22 所示。



图 8-22　“添加虚拟目录”对话框

(3) 在“别名”文本框中输入虚拟目录的名称，“物理路径”文本框中输入真实文件夹的路径，然后单击“确定”按钮，完成创建虚拟目录。在本例中，网站的主目录在 C 盘，新建的虚拟目录名为 test，将来用户如果访问该网站的 test 目录，就是在访问 E:\book 目录，这样就对用户屏蔽了路径的差异，降低了使用的难度。

(4) 创建好虚拟目录后，可以像配置网站一样配置虚拟目录。在 IIS 管理器中选中要配置的虚拟目录，此时 IIS 管理器中间的窗口显示了可以配置的项目，如图 8-23 所示。虚拟目录也可以配置主目录(也就是真实目录的路径)、默认文档、身份验证方法等，但不能为虚拟目录指定 IP 地址、端口号以及 ISAPI 筛选器。

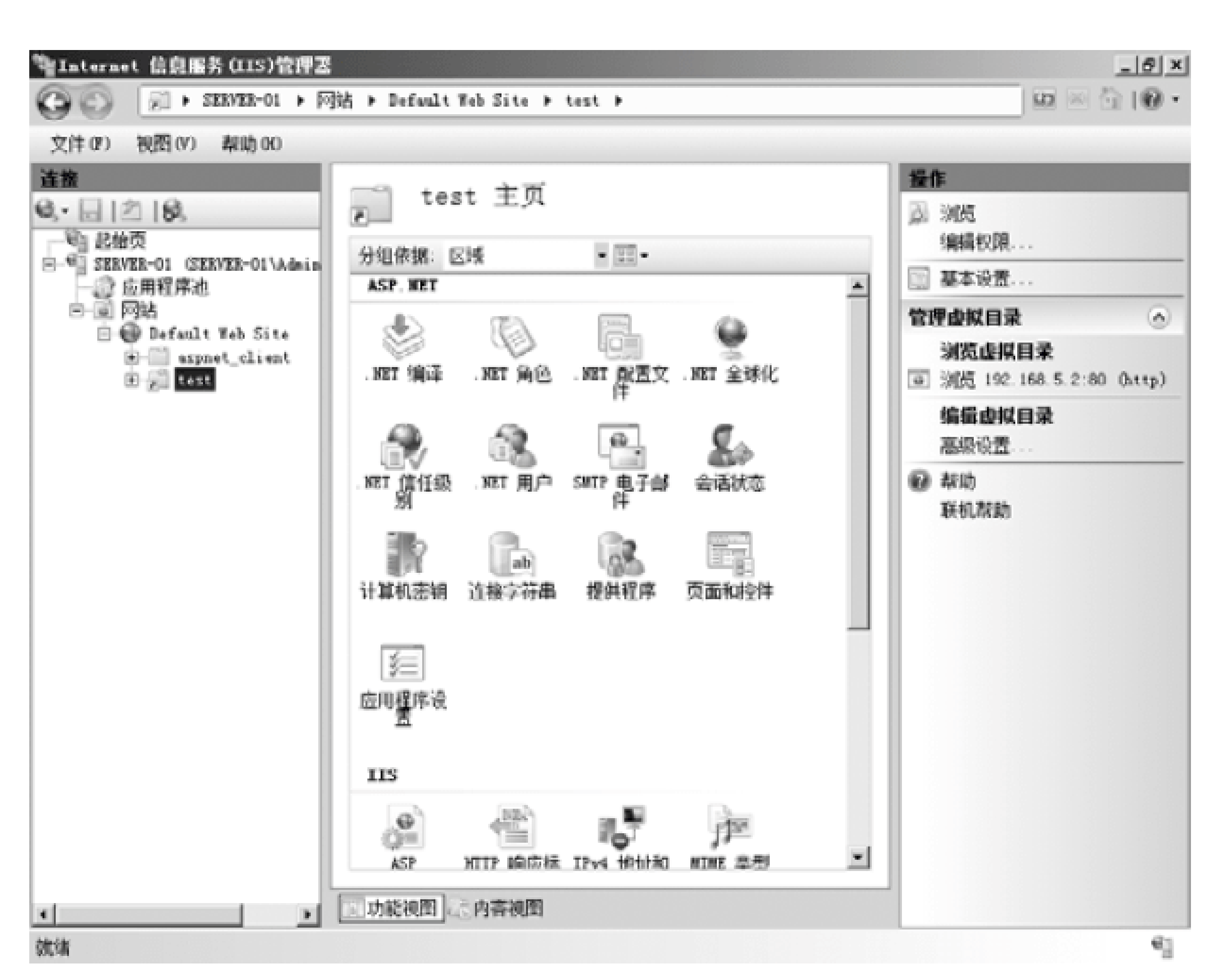


图 8-23　IIS 管理器界面

8.2.3　虚拟网站的配置

在正常情况下，一个 IP 对应着一个网站，如果想在一台服务器上运行多个网站就需要有多个 IP 地址，但这样会造成资源的极大浪费，并会使硬件平台复杂化，增加管理和维护的难度。在 Windows Server 2008 中，可以在同一台服务器，使用有限个 IP 地址的情况下，

创建多个网站，而不发生冲突。由于这些位于同一服务器上的网站在用户看起来好像是位于不同服务器，是相互独立的，因此被称为虚拟网站。

创建虚拟网站的方法如下：

(1) 在 IIS 管理器中右击“网站”节点，如图 8-24 所示。



图 8-24　IIS 管理器界面

(2) 选择“添加网站”命令，打开“添加网站”对话框，如图 8-25 所示。

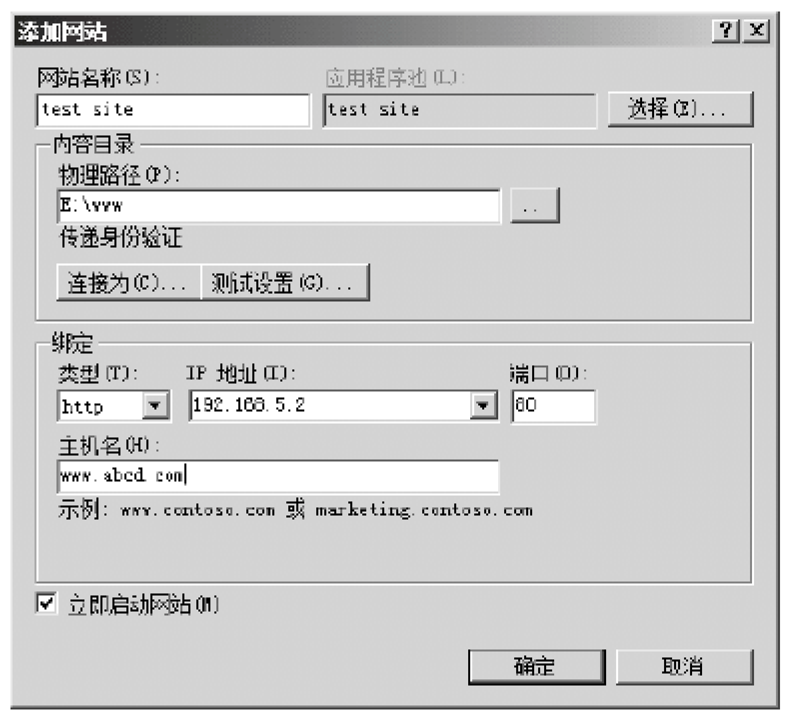


图 8-25　“添加网站”对话框

(3) 在“添加网站”对话框中，“网站名称”文本框用于输入网站的名称，该名称用于标识一个网站，便于管理员区分和管理；“物理路径”文本框用于指定该网站的主目录；“类型”选项用于指定访问该网站时使用的连接类型，“http”表示一般网站的连接方式，“https”表示使用安全连接访问网站，如使用 SSL 技术的网站；“IP 地址”文本框用于输入访问该网站时使用的 IP 地址；“端口”文本框用于输入访问该网站时使用的端口号；“主机名”文本框用于输入该网站的域名。填写完毕后，单击“确定”按钮完成创建虚拟网站。

那么，如何设置才能区分同一台服务器上的不同网站呢？有 3 种方法：一是 IP 地址，二是端口号，三是域名。因此只要一个网站的这 3 个信息中有一个和别的网站设置不同，就可以将它们区分开来。

如果一台服务器拥有多个 IP 地址，为每个虚拟网站分配一个 IP 地址即可。但这样做一般不能充分发挥服务器的性能，也不能完全利用服务器的资源。

如果一台服务器只有一个 IP 地址，为每个虚拟网站设定一个端口号即可。由于网页浏览服务的默认端口号是 80，因此当在浏览器中输入一个网站的 IP 地址或域名，浏览器就

使用 80 端口向服务器申请网页浏览服务，这个过程中用户不需要再指定使用哪个端口访问网站。如果虚拟网站的端口被配置成非 80 端口，可以将该网站和同一服务器上的其他网站区分开来，但是要注意两个问题：一是虚拟网站的端口号不能和其他服务的默认端口号冲突；二是设置完毕后，当用户访问虚拟网站时，要注明端口号，如一个虚拟网站的 IP 地址是 192.169.5.2，域名是 www.abcd.com，端口是 8000，访问时应在浏览器的地址栏中输入 http://192.168.5.2:8000，或者 http://www.abcd.com:8000。这种方法在服务器上的虚拟网站较少时可以使用，如果虚拟网站较多，如何记下不同网站的不同端口号将是一个难以解决的问题。

如果服务器只有一个 IP 地址，又不想将不同虚拟网站设置成不同的端口号，可以为不同的虚拟网站设置不同的域名，即主机名。这样做的好处是每个网站都拥有自己的主机名，便于记忆，使用方便，但前提是将所有虚拟网站的域名和 IP 地址注册到 DNS 服务器中。

8.3　搭建 SSL Web 网站

一般网站在传输数据时采用明文传送，这样的传送方式很容易导致数据被截获和篡改，这是由 HTTP 协议本身决定的。为了提高安全性，可以在服务器上配置 SSL(Secure Socket Layer，安全套接字层)。SSL 是一种利用证书对数据进行加密的技术，使用 SSL 将数据加密，然后再将加密后的数据发送给用户，用户的计算机利用证书再将数据解密，从而保证数据在传输过程中不被窃取和篡改。用户访问使用了 SSL 技术的网站时，在浏览器地址栏中要使用“https://网站地址或域名”这样的格式来访问。

8.3.1　创建 SSL 证书

SSL 是利用证书进行数据加密的，因此要使用 SSL，服务器端必须创建用于 SSL 加密的证书。证书包含了有关服务器的信息，服务器允许客户在共享敏感信息之前对其加以识别。IIS 只有安装了有效服务器证书后才能提供安全通信服务。

在 IIS 中使用 SSL 的操作步骤如下：

(1) 打开 IIS 管理器，在左侧窗口中选择服务器名称，然后在中间窗口找到“服务器证书”图标并双击，打开“服务器证书”窗口，如图 8-26 所示。

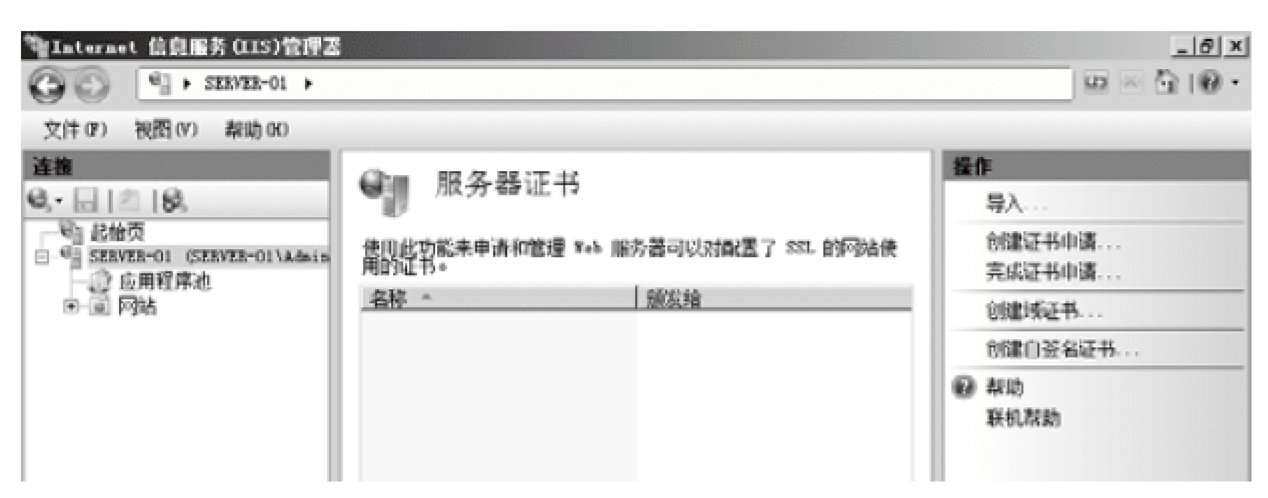


图 8-26　“服务器证书”界面

(2) 目前还没有任何证书，如果服务器上保存有以前创建好的证书，可以单击“导入”选项将以前的证书导入到 IIS 中。如果以前没有证书，单击“创建证书申请”，可以向有关认证机构申请证书。也可以单击“创建自签名证书”，打开“创建自签名证书”对话框，如图 8-27 所示。



图 8-27　“创建自签名证书”对话框

(3) 输入证书的名称后，单击“确定”按钮，证书创建完毕，并自动导入到 IIS，显示在证书列表中，如图 8-28 所示。



图 8-28　“服务器证书”界面

(4) 选中创建好的证书，单击右侧窗口的“查看”，打开“证书”对话框，如图 8-29 所示。在该对话框中，显示了证书的名称、颁发者、颁发给、到期日期和证书哈希等信息。

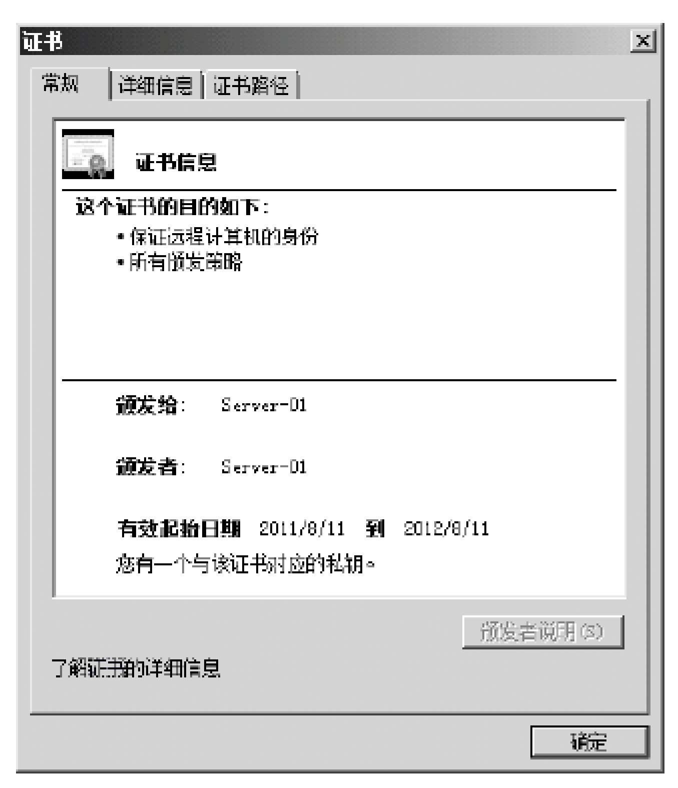


图 8-29　“证书”对话框

8.3.2　创建 SSL 网站

创建完 SSL 证书并导入 IIS 以后，就可以创建 HTTPS 网站了。但是不能先创建 HTTP 网站，再创建 SSL 证书，然后将 HTTP 网站的通信协议改为 HTTPS。

创建 HTTPS 网站的步骤如下：

(1) 打开 IIS 管理器，在左侧窗口中的“网站”节点上右击，在弹出的快捷菜单中选择“添加网站”命令，打开“添加网站”对话框，如图 8-30 所示。

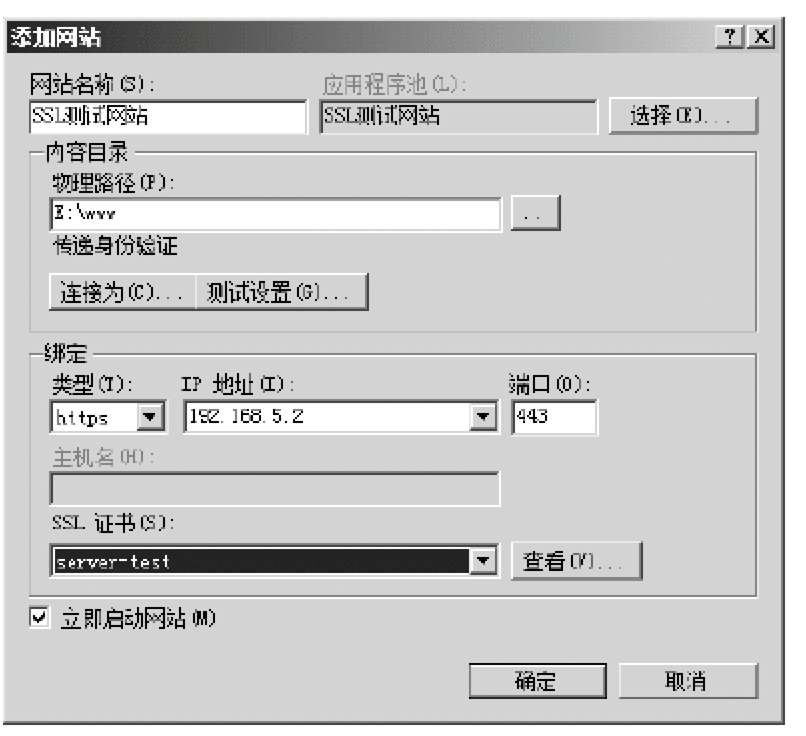


图 8-30　“添加网站”对话框

(2) 需要输入的主要内容和创建虚拟网站时一样，这里不再赘述。需要注意的是，“类型”应选择为“https”，端口不要修改，使用默认的“443”端口，这是 HTTPS 使用的端口，和 HTTP 使用的 80 端口不同；“SSL 证书”则从下拉列表中选择创建好的 SSL 证书。然后单击“确定”按钮完成网站创建。

(3) 在 IIS 左侧窗口中选中创建好的 HTTPS 网站，在中间窗口中双击“SSL 设置”图标，打开“SSL 设置”界面，如图 8-31 所示。



图 8-31　“SSL 设置”界面

(4) 选中“要求 SSL”复选框，此时启用 SSL 加密数据，但是采用的是安全性较低的 40 位加密方法，如果想提高数据安全性，可以再选中“需要 128 位 SSL”复选框。在“客户证书”选项中，有 3 个选项可供选择。

- 忽略：系统默认设置，如果提供客户端证书，则不会被接受，也就是说，没有安全

验证，这种设置安全性最低。

- 接受：启用服务器端的 SSL 设置，并接受客户端证书，在允许客户端获得内容访问权限之前验证客户身份。建议采用此选项。
- 必需：在接受访问之前客户端必须提供证书，用于验证客户端的身份是否合法，安全性最高。

(5) 设置完毕后，单击右侧窗口的“应用”，完成设置。

8.3.3　访问 SSL 网站

用户访问 SSL 网站与访问普通网站稍有不同。首先，使用 SSL 技术的网站的网址是以 https://开头的；第二，用户必须能够连接到站点指定的证书服务器，以获取相应的证书。其他方面和访问普通网站相同，这里不再赘述。

8.4　本章小结

本章介绍了如何在 Windows Server 2008 上使用 IIS 7 搭建网站的基本方法，通过 IIS，用户可以自己搭建网站，对外发布信息，实现对外的信息交流。如果用户对安全性要求较高，则可以限制访问的帐户和 IP 地址，也可以使用 SSL 协议提高网站的安全性。

(1) Web 服务的搭建与配置：本节介绍了安装和简单配置 IIS 的方法，通过本节学习，学生可以掌握使用 IIS 搭建网站的基本方法，并可以启动、停止和重启网站。

(2) Web 服务器的管理：本节介绍了 IIS 的基本管理，通过本节学习，学生可以控制访问网站的身份和 IP 地址，限制不安全因素，提升网站安全性，还可以创建虚拟目录和虚拟站点，在同一台服务器上设置多个目录和站点，提高硬件的利用效率。

(3) 搭建 SSL Web 网站：本节介绍了网站通过采用 SSL 技术提高安全性的方法，通过本章学习，学生可以使用 SSL 协议搭建更加安全的网站，访问使用了 SSL 协议的安全网站。

8.5　思考与练习

【思考题】

1. 创建虚拟站点的意义是什么？
2. 如何提高网站的安全性？
3. 什么是主目录，什么是虚拟目录，两者有什么联系？
4. 如果创建网站时没有指定默认文档，是否可以访问这个网站中的网页？该如何访问？

【练习题】

1. 创建网站的虚拟目录(参考 8.2.2 节)。
2. 为网站 SSL 安装数字证书(参考 8.3.1 节)。

第9章　FTP服务

【本章导读】

FTP服务是网络中历史最悠久也是最常见的服务之一，尤其是在局域网中，因具有速度快、安全性好的优点，是文件共享的首选方式。Windows Server 2008 中的 IIS 组件不仅可以提供 Web 服务，还可以提供 FTP 服务。即允许客户下载服务器上的文件，也允许客户上传文件到服务器，还可以通过 FTP 服务来维护 Web 网站中的文件。

9.1　FTP 服务器的安装与配置

FTP(File Transfer Protocol)是文件传输协议的简称，是一种在网络中不同计算机系统之间传输文件的协议。通过 FTP 服务，客户可以从服务器上下载文件，也可以将自己的文件上传至服务器和其他客户共享。

9.1.1　FTP 服务的安装

在 Windows Server 2008 中，FTP 在默认状态下并没有安装，也不是一个独立的服务，而是 IIS 中的一个服务组件。要使服务器提供 FTP 服务，首先要安装相关组件。前面章节中已经安装了 IIS 7，本章在此基础上添加 FTP 组件。步骤如下：

(1) 打开服务器管理器，选择左侧窗口中的“角色”节点，然后单击右侧窗口中“Web 服务器(IIS)”右侧的“添加角色服务”，打开添加角色向导，如图 9-1 所示。

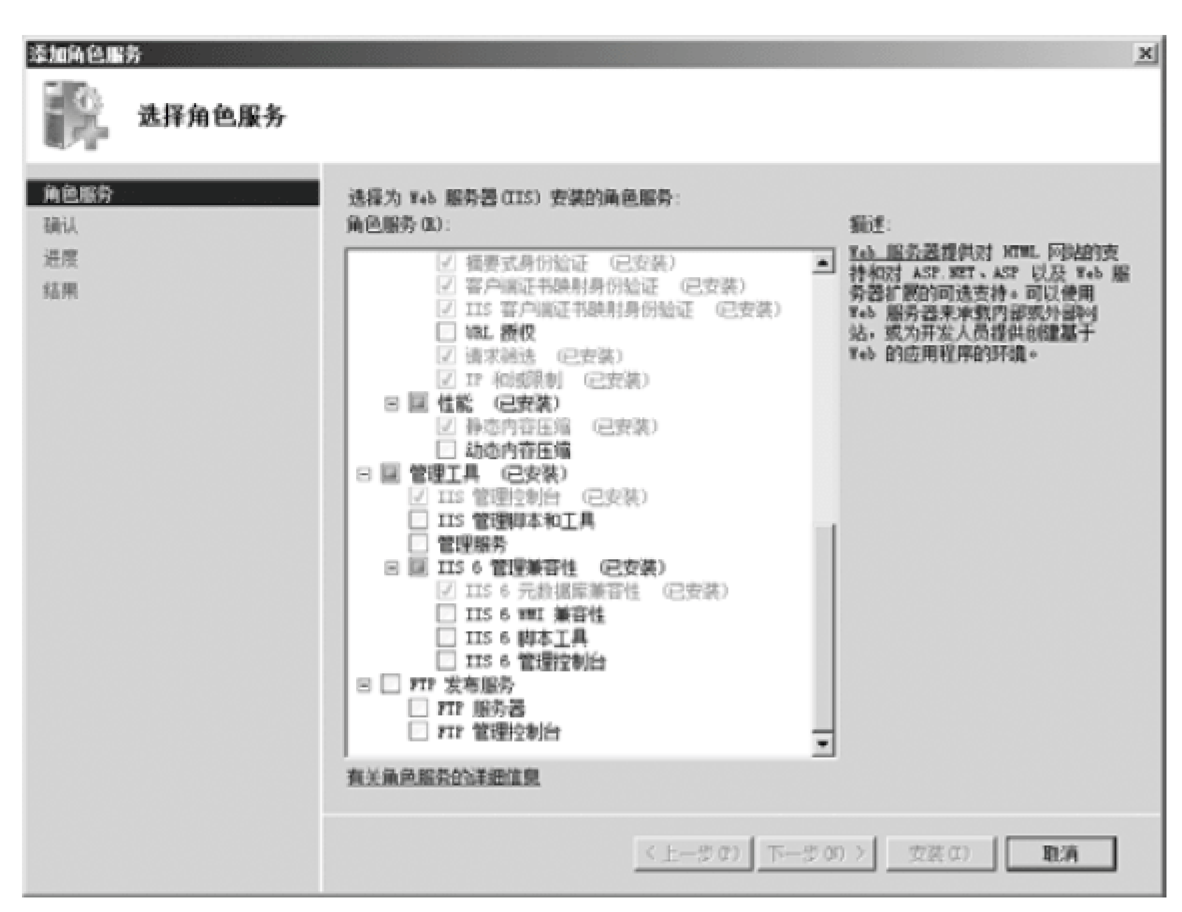


图 9-1　“选择角色服务”界面

(2) 选中最下方的“FTP 发布服务”及其子项，其间会有对话框提示要安装 IIS6 的兼容组件，单击“添加必需的角色服务”按钮即可。然后单击“下一步”按钮，进入“确认”界面，单击“安装”按钮，等待几分钟后，安装完毕。

Windows Server 2008 系统的 IIS 7 中并没有 FTP 服务，因此在安装 FTP 功能时要安装老版本的 IIS 6 管理工具，将来对 FTP 服务进行配置时也是在 IIS 6 管理界面下完成的。

9.1.2　FTP 服务的基本配置

FTP 服务安装好后，系统中已经有了一个 FTP 站点，本节以此站点为例讲解 FTP 服务的基本配置。步骤如下：

(1) 依次选择“开始”→“管理工具”→“Internet 信息服务(IIS)6.0 管理器”，展开 FTP 站点，如图 9-2 所示。



图 9-2　“IIS6.0 管理器”界面

(2) 在默认站点“Default FTP Site”上右击，在弹出的快捷菜单中选择“启动”命令，启动该 FTP 站点。如果在站点上右击，在弹出的快捷菜单中选择“停止”命令，则可以停止 FTP 站点的运行。在启动后的站点上右击，在弹出的快捷菜单中选择“属性”命令，打开 FTP 站点的属性对话框，如图 9-3 所示。

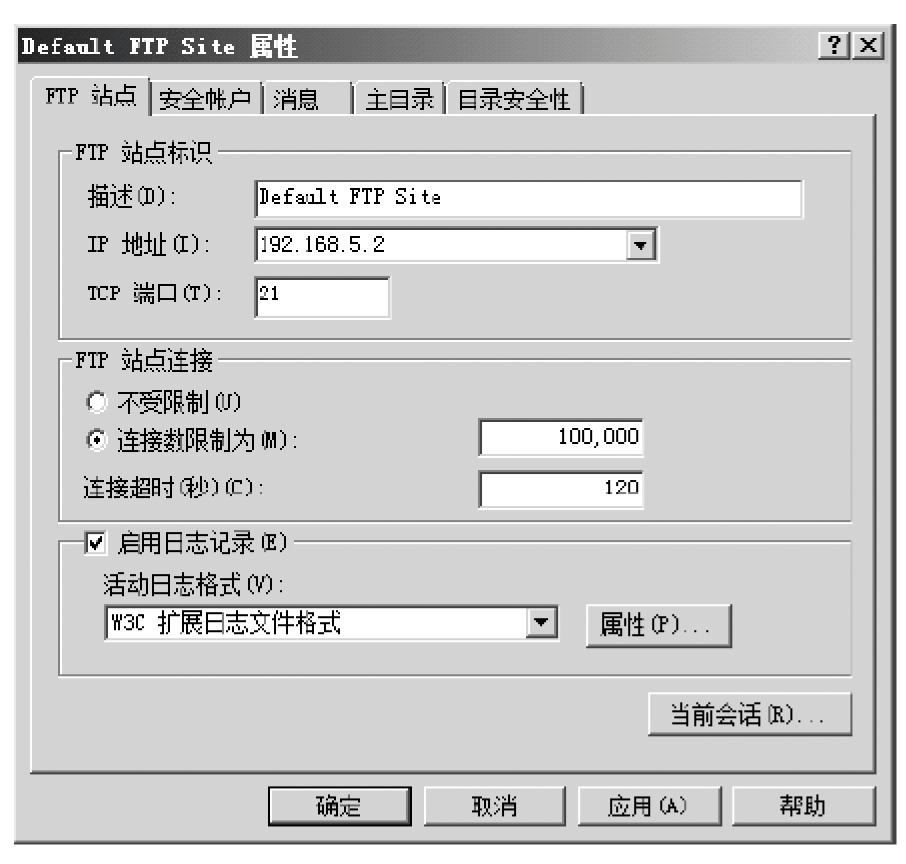


图 9-3　“FTP 站点”选项卡

(3) 在“FTP 站点”选项卡中，可以设置 FTP 站点的基本信息。具体设置选项如下。

- “描述”文本框：设置该 FTP 站点的名称，仅供管理员管理区分不同的站点。

- “IP 地址”下拉列表框：默认情况下显示“全部未分配”，管理员可以单击下拉列表框，从中选择一个服务器的 IP 地址分配给当前的 FTP 站点，将来用户可以使用分配好的 IP 地址访问该站点。
- “TCP 端口”文本框：用于设置访问当前 FTP 站点时使用的端口号。FTP 服务的默认端口是 21。
- “FTP 站点连接”选项组：FTP 服务用于在网络上传输文件，如果有多个用户同时使用 FTP 传输文件，会占用大量系统资源和网络带宽，影响了服务器上其他服务的正常运行。尤其是在一些中小企业中，由于成本控制需要，往往在一台服务器上运行了 WWW 服务、FTP 服务、电子邮件服务等，如果 FTP 服务占用了过多的计算机资源和带宽，会导致其他服务不能正常运行。因此，可以对网络上的通信连接进行限制。如果不需要对连接数进行设置，选择“不受限制”选项；如果需要限制连接数，选择“连接数限制为”选项，并在其后文本框中输入最大连接数，当连接数超过最大连接数时，服务器会对后来的连接请求进行限制；有时会有用户连接到服务器后却不释放连接，这对后来申请连接的用户会有不良影响，因此应当选择“连接超时”，并在对应的文本框中输入一个时间，当用户连接到 FTP 服务器后，若在指定时间内没有任何动作，服务器则自动释放该连接。

(4) 设置完“FTP 站点”选项卡后，单击打开“消息”选项卡，如图 9-4 所示。



图 9-4　“消息”选项卡

(5) “消息”选项卡用于设置登录信息，当用户登录、退出或无法连接时给出相应的提示信息，各选项的作用分别如下。

- “横幅”文本框：用户连接到 FTP 服务器时所显示的信息，通常是 FTP 站点的名称。
- “欢迎”文本框：用户连接到服务器后所显示的信息，通常包括向用户致意、使用该 FTP 站点时应注意的问题、管理者的联系方式、上传下载的规则说明等信息。
- “退出”文本框：当用户从 FTP 服务器退出时显示的信息，通常是欢迎再次访问等内容。

- “最大连接数”文本框：当连接到服务器的连接数已达服务器设置的上限，还继续有用户连接时会导致连接失败，此时服务器将向用户说明情况并显示提示信息。

(6) 配置完毕后，单击打开“主目录”选项卡，如图 9-5 所示。

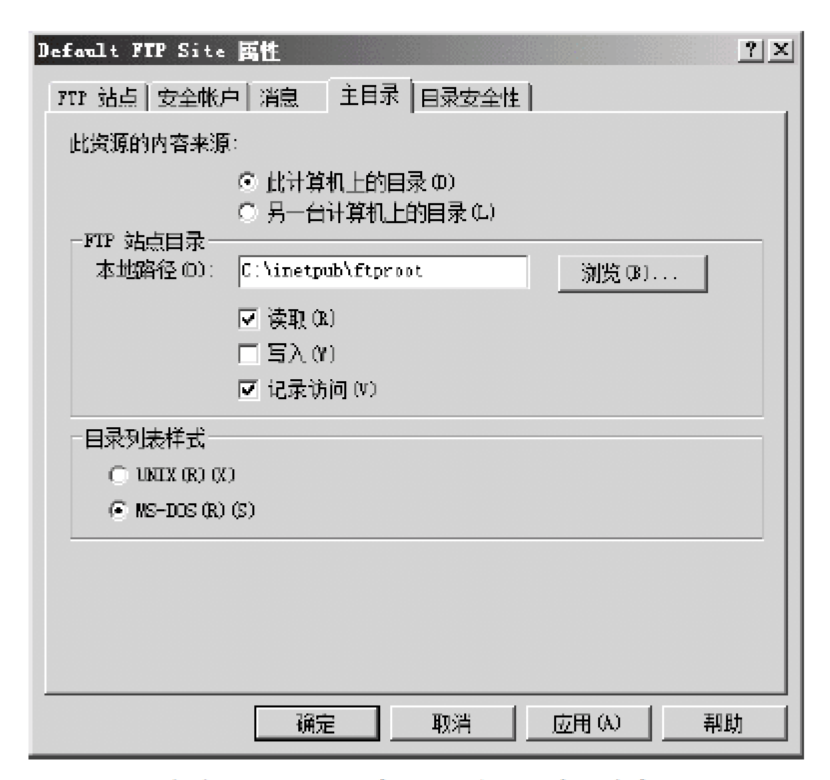


图 9-5　“主目录”选项卡

(7) “主目录”选项卡用于设置 FTP 站点的根目录，即保存 FTP 站点中所有文件夹和文件的目录，一般在服务器本地磁盘中，也可以设置到另一台计算机上的磁盘中。当用户访问 FTP 站点时，实际上就是访问 FTP 站点的主目录。首先选中“此计算机上的目录”，然后在“FTP 站点目录”的“本地路径”文本框中输入主目录路径，然后根据需要选择“读取”和“写入”权限。选中“读取”复选框，表示用户可以从服务器上下载文件或文件夹；选择“写入”复选框，表示用户可以向服务器上传文件或文件夹；选择“记录访问”复选框，表示开启日志功能，所有活动都将记录入日志。设置完毕后，单击“确定”按钮，完成 FTP 站点的基本设置。

9.2　为 FTP 设置 NTFS 访问权限

IIS 中对 FTP 站点的权限设置选项较少，只有读取和写入两种，并且默认本地服务器和域中所有用户都具有访问权限。为了提高权限设置的灵活性，管理员可以将 FTP 服务器与 NTFS 文件系统的权限管理结合起来，从而进行更细致的权限设置，以满足不同用户的需求。

9.2.1　取消继承关系

为了提高 FTP 站点主目录的安全性，首先应当将能够访问主目录而又非 IIS 指定的用户删除。但是 FTP 站点的主目录往往是某个目录的子目录，或者某个卷的目录，这样它会从父目录或者所在卷继承一些 NTFS 权限，即子目录的 NTFS 权限和父目录的 NTFS 权限设置是相同的，这就导致某些无关用户是无法从子目录的权限设置中排除掉的。如果想排

除这些无关用户，首先要取消不同层次目录之间的权限继承关系。操作方法如下：

(1) 打开资源管理器，在 FTP 站点主目录(或虚拟目录对应的物理目录)上右击，从弹出的快捷菜单中选择“属性”命令，打开“属性”对话框，单击打开“安全”选项卡，如图 9-6 所示。

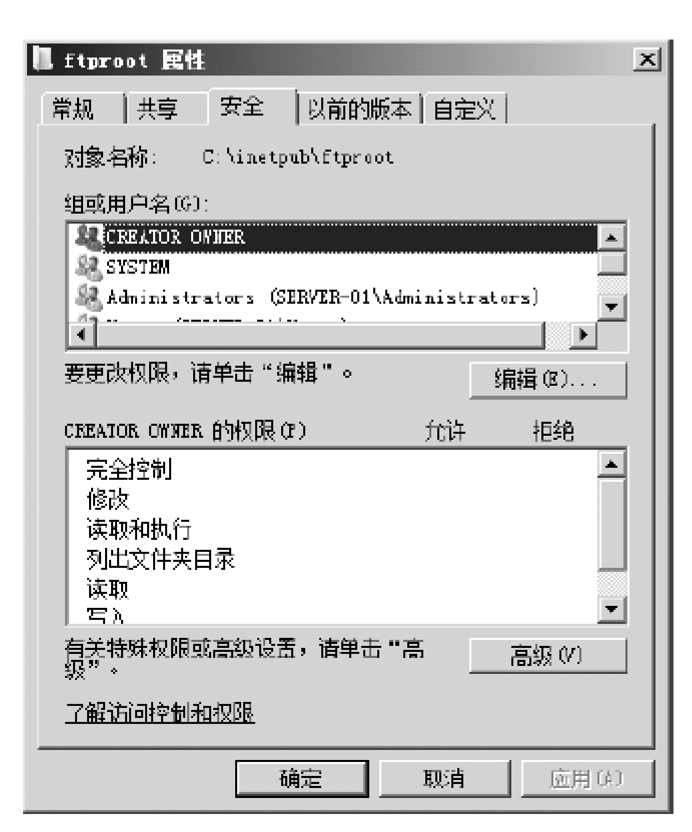


图 9-6　“安全”选项卡

(2) 单击“高级”按钮，打开“高级安全设置”对话框，如图 9-7 所示。

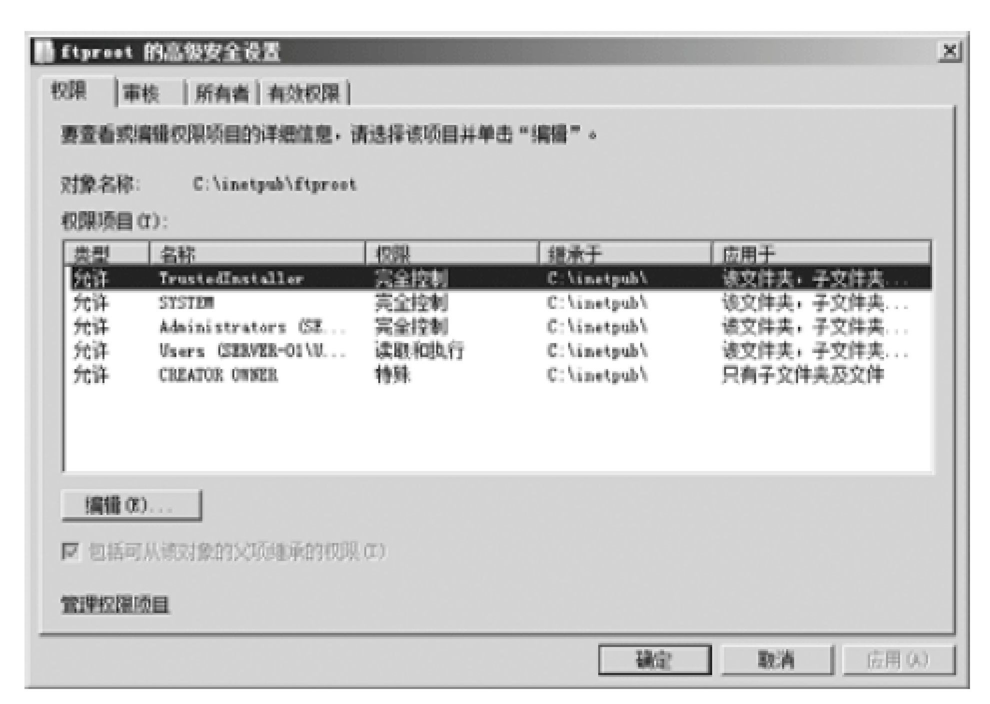


图 9-7　“高级安全设置”对话框

(3) 单击“编辑”按钮，打开编辑界面，对话框下方显示两个复选框，如图 9-8 所示。

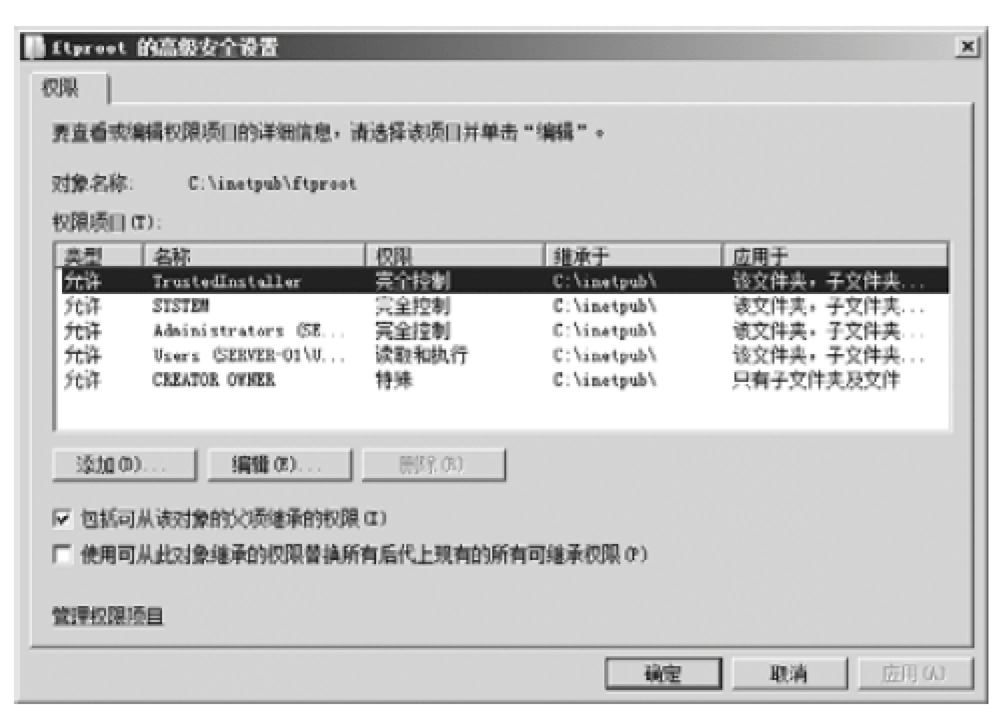


图 9-8　“高级安全设置”对话框的编辑界面

(4) 取消选中的“包括可从该对象的父项继承的权限”复选框，会弹出“Windows 安全”对话框，询问是否取消继承，如图 9-9 所示。

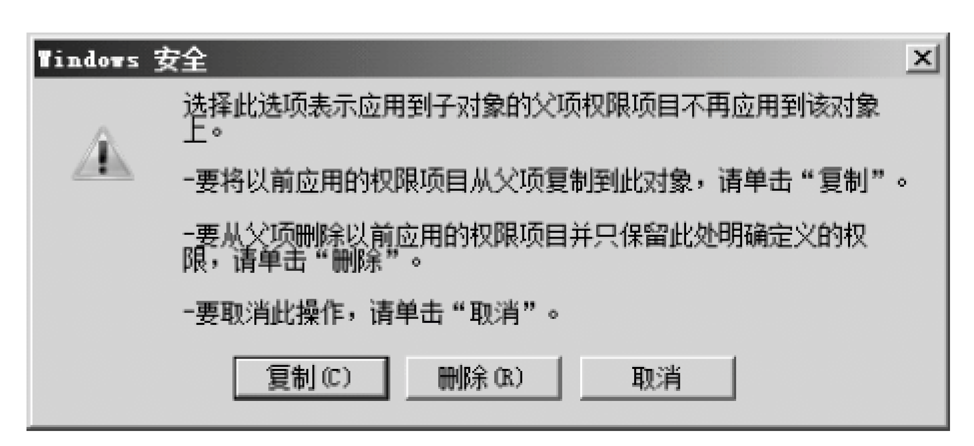


图 9-9　“Windows 安全”对话框

(5) 单击“删除”按钮，确认删除权限继承，此时“权限项目”一栏中所有的用户均被取消，如图 9-10 所示。



图 9-10　删除权限后的“高级安全设置”对话框

(6) 单击“确定”按钮，会弹出“Windows 安全”对话框，询问是否要继续取消所有用户的权限，如图 9-11 所示。

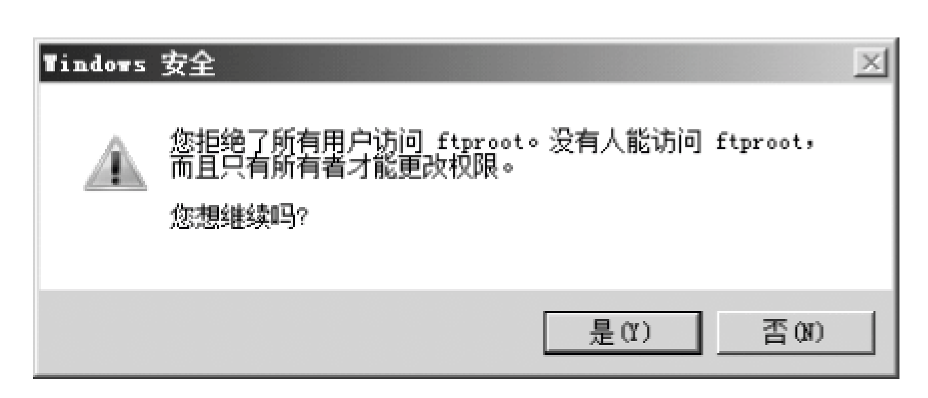


图 9-11　“Windows 安全”对话框

(7) 单击“是”按钮，返回“高级安全设置”对话框，再单击“确定”按钮，返回到“安全”选项卡，单击“确定”按钮关闭对话框。再次打开该目录的“属性”对话框中的“安全”选项卡，其中没有任何用户拥有对该目录进行操作的权限，如图 9-12 所示。

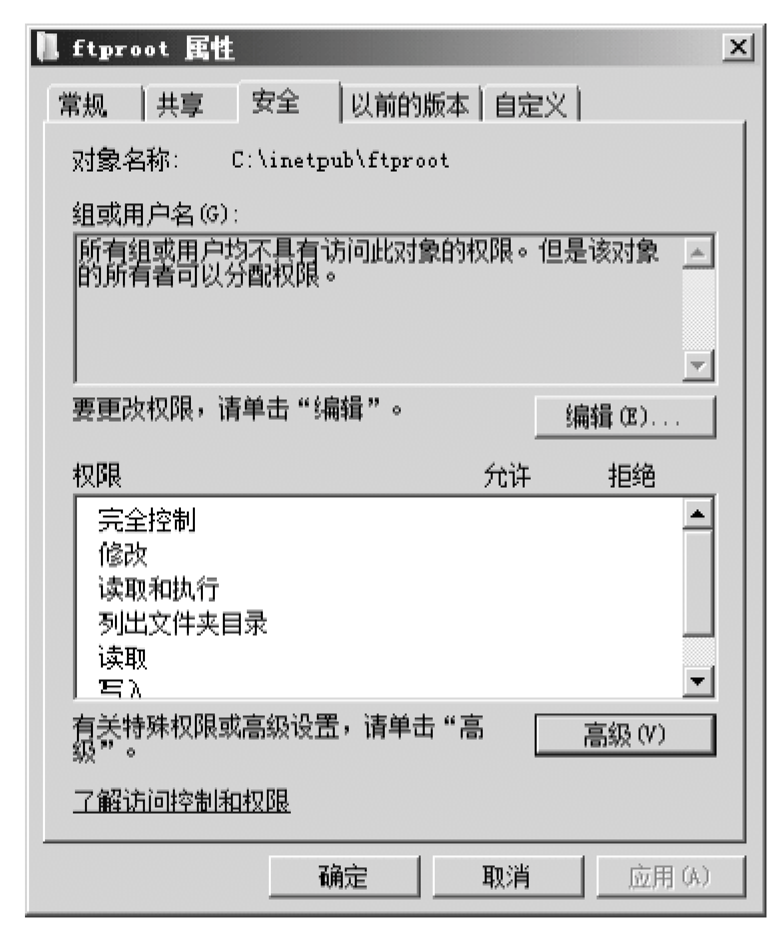


图 9-12　“安全”选项卡

至此，已经将无关用户排除掉了，下面就可以开始对相关用户进行权限设置了。

9.2.2　设置用户权限

经过上面的操作，只有系统管理员拥有为该目录分配 NTFS 权限的权限。操作方法如下：

(1) 打开图 9-12 所示的对话框，单击“编辑”按钮，打开相应目录的“权限”对话框，如图 9-13 所示。

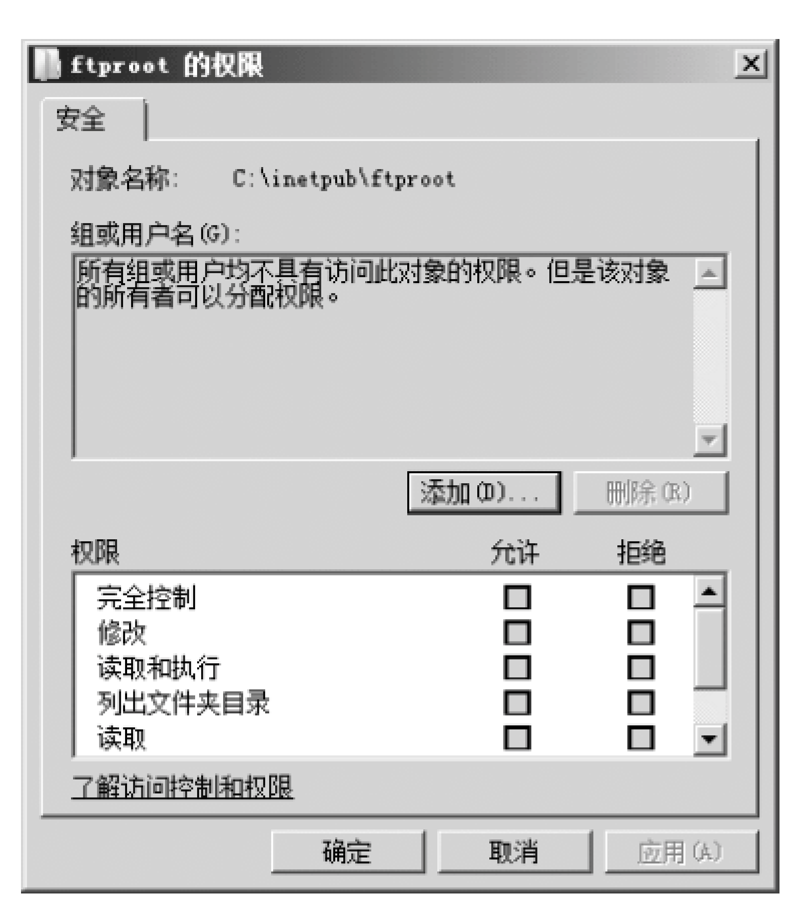


图 9-13　“ftproot 的权限”对话框

(2) 单击“添加”按钮，打开“选择用户和组”对话框，并单击其中的“高级”按钮，然后单击“立即查找”按钮，对话框中列出当前系统中所有可用的用户和组，如图 9-14 所示。

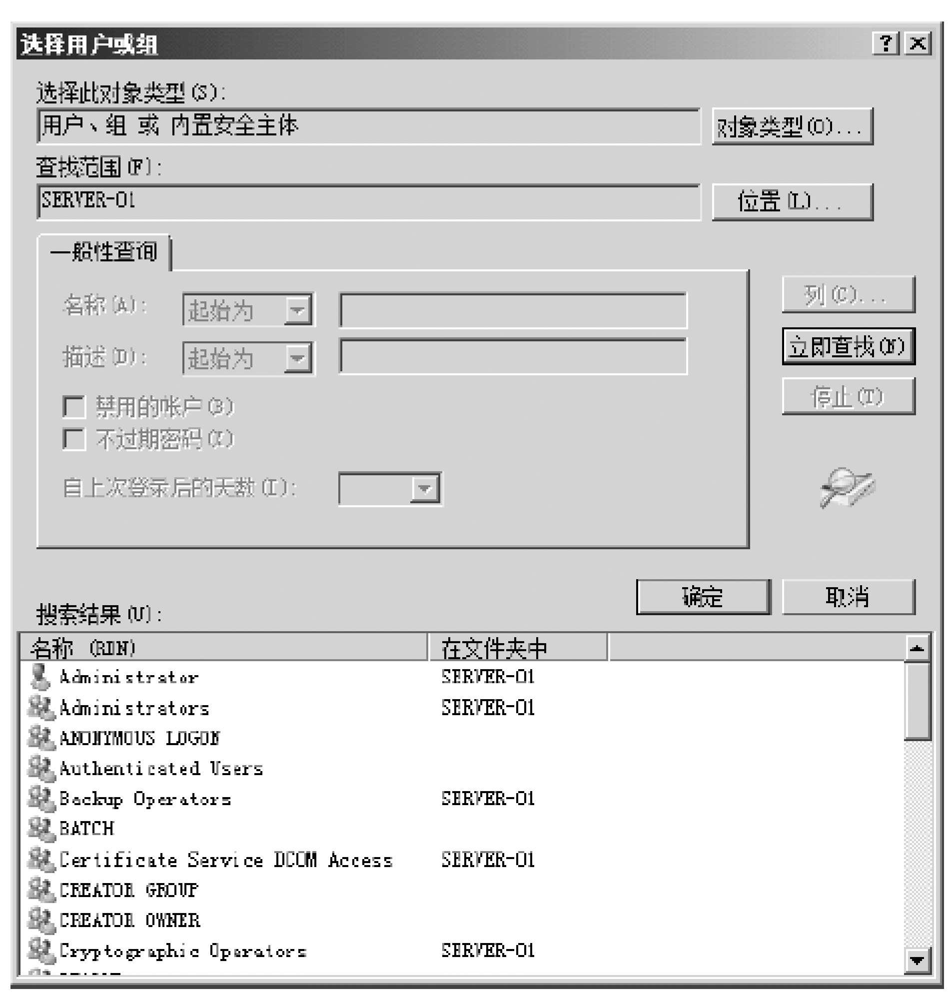


图 9-14　“选择用户和组”对话框

(3) 在“搜索结果”列表框中选择管理员(Administrator)和 Internet 来宾帐户(IUSR_SERVER. 01)，选择时可以按下 Ctrl 键同时选择用户名，这样可以同时选择多个用户。选择完毕后，单击“确定”按钮，返回“选择用户和组”对话框，如图 9-15 所示。



图 9-15　“选择用户和组”对话框

(4) 单击“确定”按钮，返回“ftproot 的权限”对话框，如图 9-16 所示。



图 9-16　“ftproot 的权限”对话框

(5) 在该对话框中可以为每个用户设置访问 FTP 主目录的权限。每个用户都有 6 个权限选项可供选择，分别是完全控制、修改、读取和执行、列出文件夹目录、读取和写入，分别有允许和拒绝两种状态。选中相应的复选框，单击“确定”按钮即可完成配置。一般来说，管理员帐户可以设置为“完全控制”，这样可以对 FTP 站点主目录进行方便的操作；Internet 来宾帐户则根据 FTP 站点为用户设置的权限进行相应的设置。

(6) 如果想对该目录进行更详细的设置，可以在返回到“安全”选项卡后，单击其中的“高级”按钮，在打开的“高级安全设置”对话框中单击“编辑”按钮，打开高级安全设置界面，如图 9-17 所示。

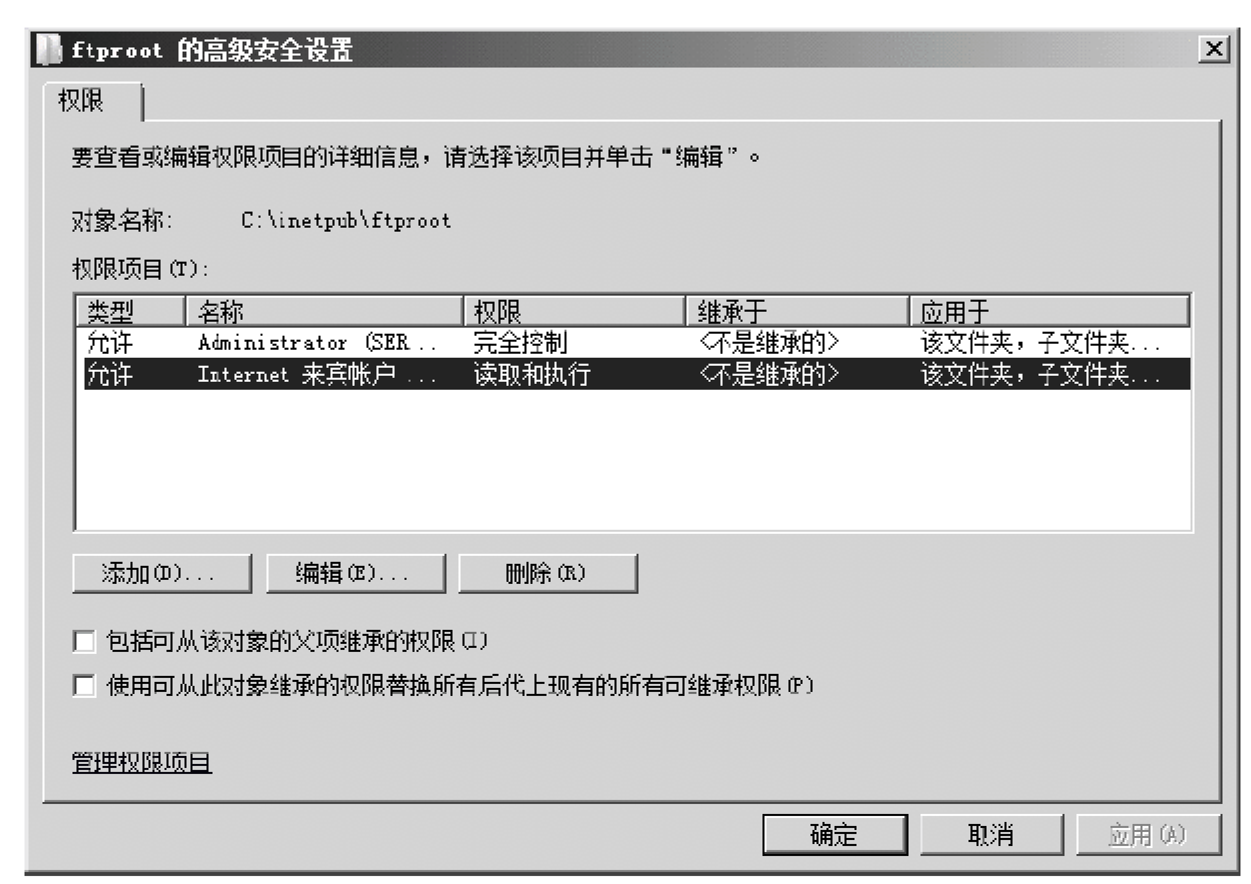


图 9-17　“高级安全设置”对话框

(7) 选中一个用户，然后单击“编辑”按钮，打开“权限项目”对话框，如图 9-18 所示。该对话框中有 14 种权限可供选择，以便进行更加详细的设置。

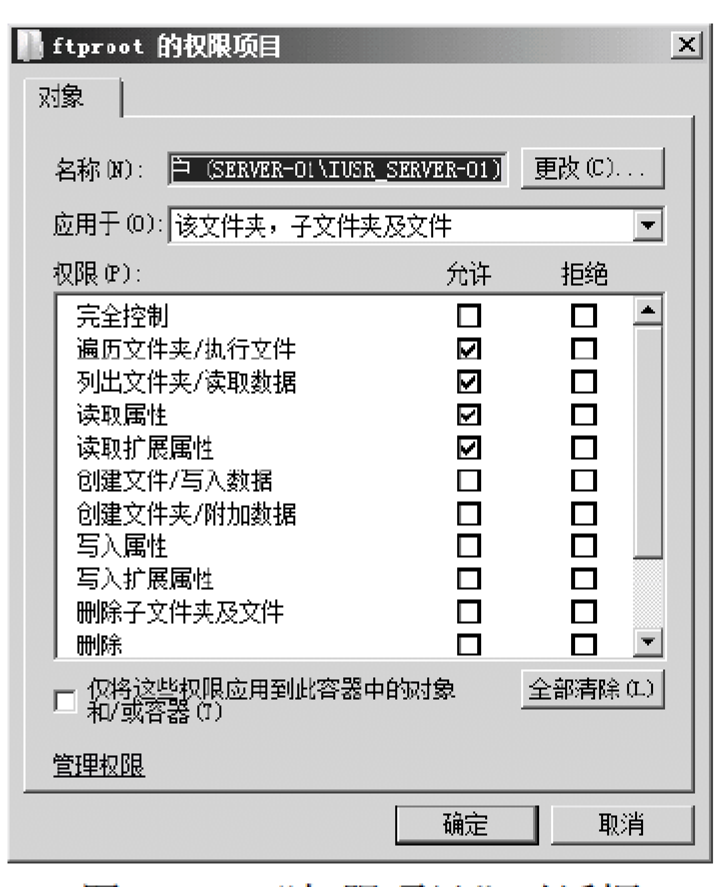


图 9-18　“权限项目”对话框

(8) 设置完毕后，单击“确定”按钮，完成设置。

利用 NTFS 权限和 FTP 站点分配权限相结合的方式，可以进行更加详细的设置，从而

更好地实现来访用户的访问控制。

9.2.3　FTP 空间使用限制

FTP 服务可以提供文件的上传和下载，允许用户从服务器下载文件的同时也可以允许用户上传文件到服务器。如果用户上传文件过多，占用磁盘空间过大，会导致 FTP 站点主目录所在的卷空间不足，影响 FTP 或其他服务的正常运行，因此开启了上传权限的 FTP 站点应当启用空间限制功能。

IIS 中的 FTP 服务没有空间限制功能，因此要实现该功能只能借助于 NTFS 文件系统的磁盘配额功能。需要注意的是，在微软公司的操作系统使用的文件系统中，只有 NTFS 文件系统可以支持磁盘配额，FAT 和 FAT32 等文件系统不支持磁盘配额，所以要实现对用户上传空间的限制，必须将 FTP 主目录(包括虚拟目录)放置于采用 NTFS 文件系统的卷上。

具体操作方法如下：

(1) 打开资源管理器，在 FTP 主目录(或虚拟目录)所在的卷上右击，从弹出的快捷菜单中选择“属性”命令，再打开“配额”选项卡，如图 9-19 所示。

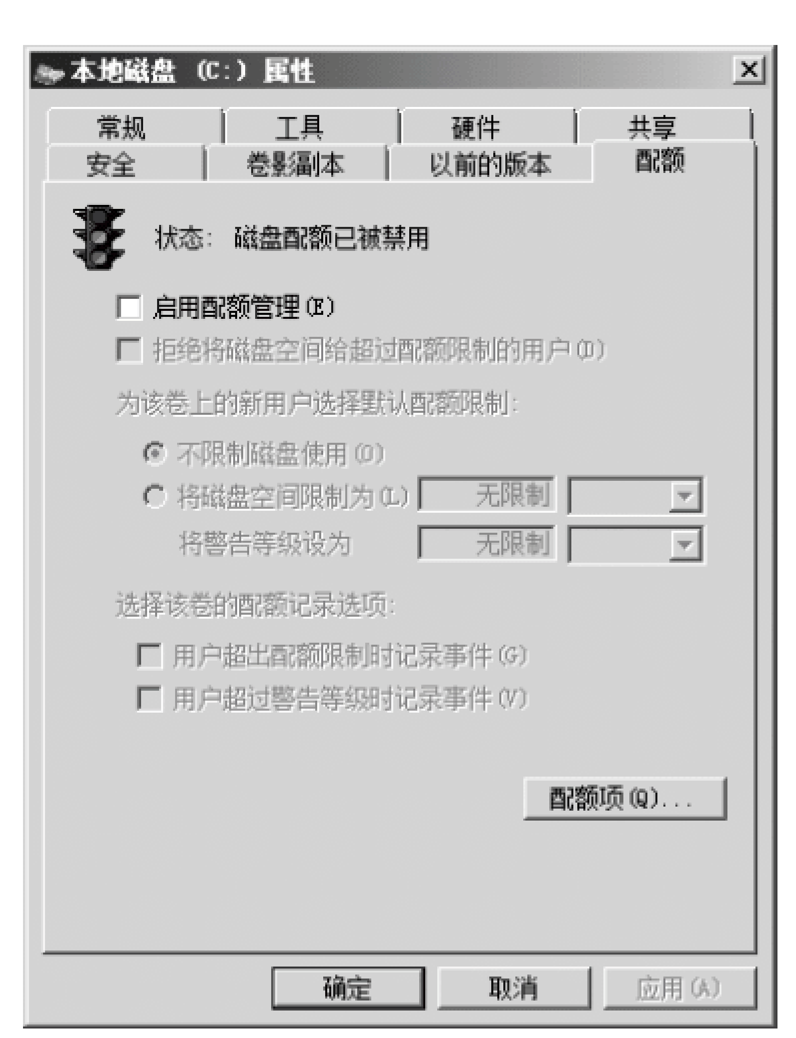


图 9-19　“配额”选项卡

(2) 选中“启用配额管理”复选框，如图 9-20 所示。默认状态下是不限制磁盘空间的，因此要选中“将磁盘空间限制为”单选按钮，再进行配置。“将磁盘空间限制为”文本框中要输入一个用户可以使用的最大磁盘空间，后面的下拉列表框是空间的单位，“将警告等级设为”文本框要输入一个空间大小，这个值不能超过“将磁盘空间限制为”文本框中所输入的数值，否则将失去应有的作用，当用户使用的空间超过这个值时，向用户发出警告。

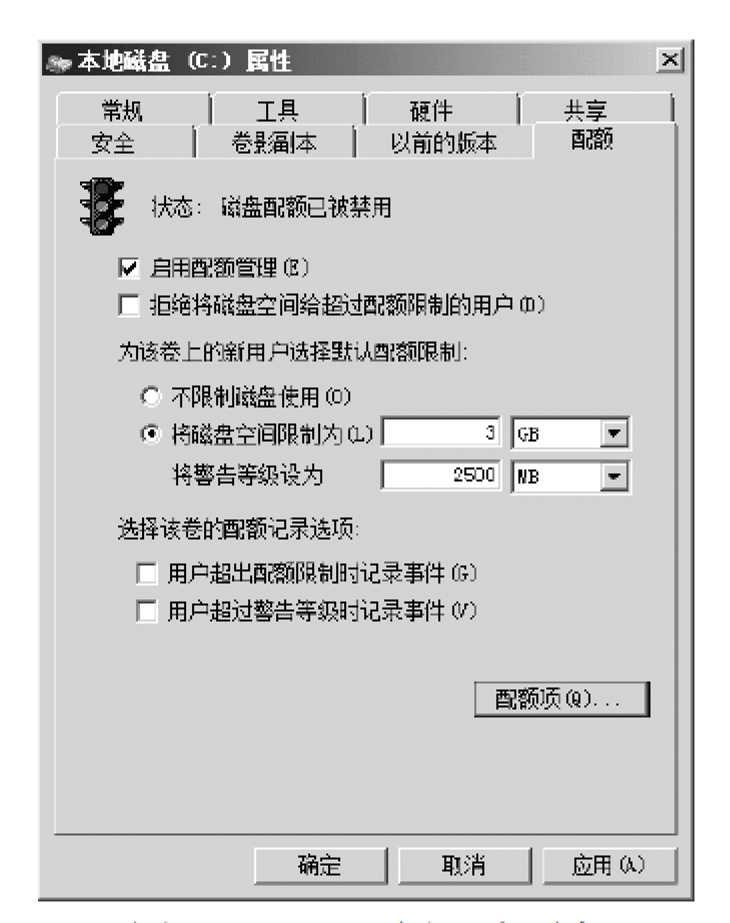


图 9-20　“配额”选项卡

(3) 设置完毕后，单击“确定”按钮关闭对话框。

9.3　虚拟站点与虚拟目录

9.3.1　虚拟站点

和 Web 服务一样，IIS 中的 FTP 服务也提供了虚拟站点功能，可以在一台服务器上提供多个 FTP 站点，还可以对不同的 FTP 站点进行单独管理和配置，可以拥有不同的 IP 地址和端口号，可以为不同的用户设置不同的权限，这些站点从用户的角度看就是相互独立的。这样就大大提高了服务器的利用率。

设置虚拟站点方法如下：

(1) 打开 IIS 6 管理器。在左侧窗口上的“FTP 站点”节点上右击，在弹出的快捷菜单中选择“新建”→“FTP 站点”命令，打开 FTP 站点创建向导，如图 9-21 所示。

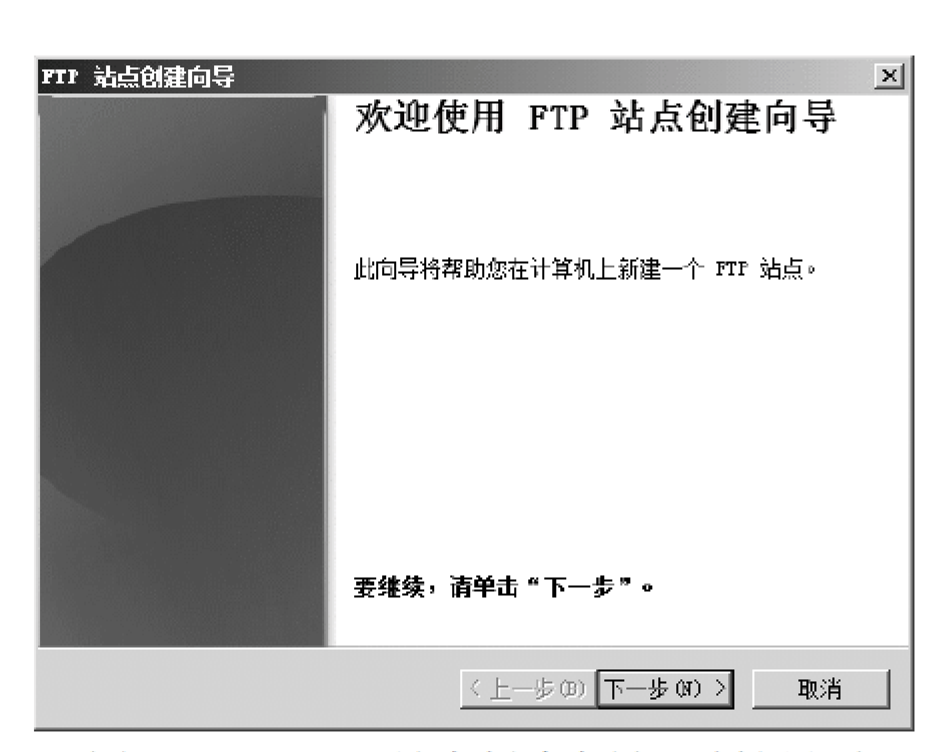


图 9-21　“FTP 站点创建向导”欢迎界面

(2) 单击“下一步”按钮，进入“FTP 站点描述”界面，如图 9-22 所示。



图 9-22　“FTP 站点描述”界面

(3) 在“描述”文本框中输入对 FTP 站点的描述，也就是该站点的名称。此处的描述信息对 FTP 服务本身没有影响，仅供管理员维护使用。设置完毕后，单击“下一步”按钮，进入“IP 地址和端口设置”界面，如图 9-23 所示。

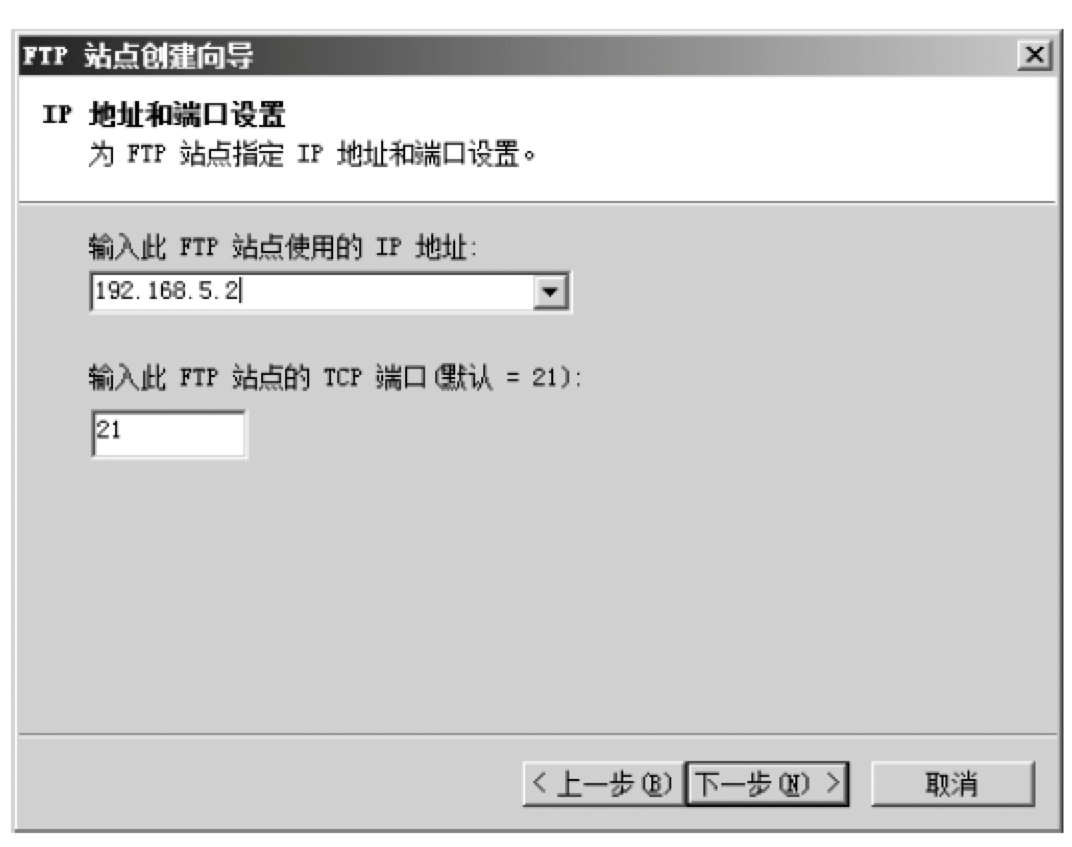


图 9-23　“IP 地址和端口设置”界面

(4) 在“输入此 FTP 站点使用的 IP 地址”下来列表中选择一个 IP 供 FTP 站点使用，如果要设置多个站点，可以在此下拉列表中选择不同的 IP 地址分配给每个站点，这样就可以通过不同的 IP 地址访问不同的 FTP 站点；在“输入此 FTP 站点的 TCP 端口”文本框中输入当前 FTP 站点提供服务时使用的端口号，默认的端口号为 21。如果服务器拥有的 IP 地址有限，但是服务器上的 FTP 站点较多，可以为多个 FTP 站点分配一个 IP 地址，但是不同的站点最好分配不同的端口号，这样可以通过不同的端口访问不同的站点。设置完毕后，单击“下一步”按钮，进入“FTP 用户隔离”界面，如图 9-24 所示。

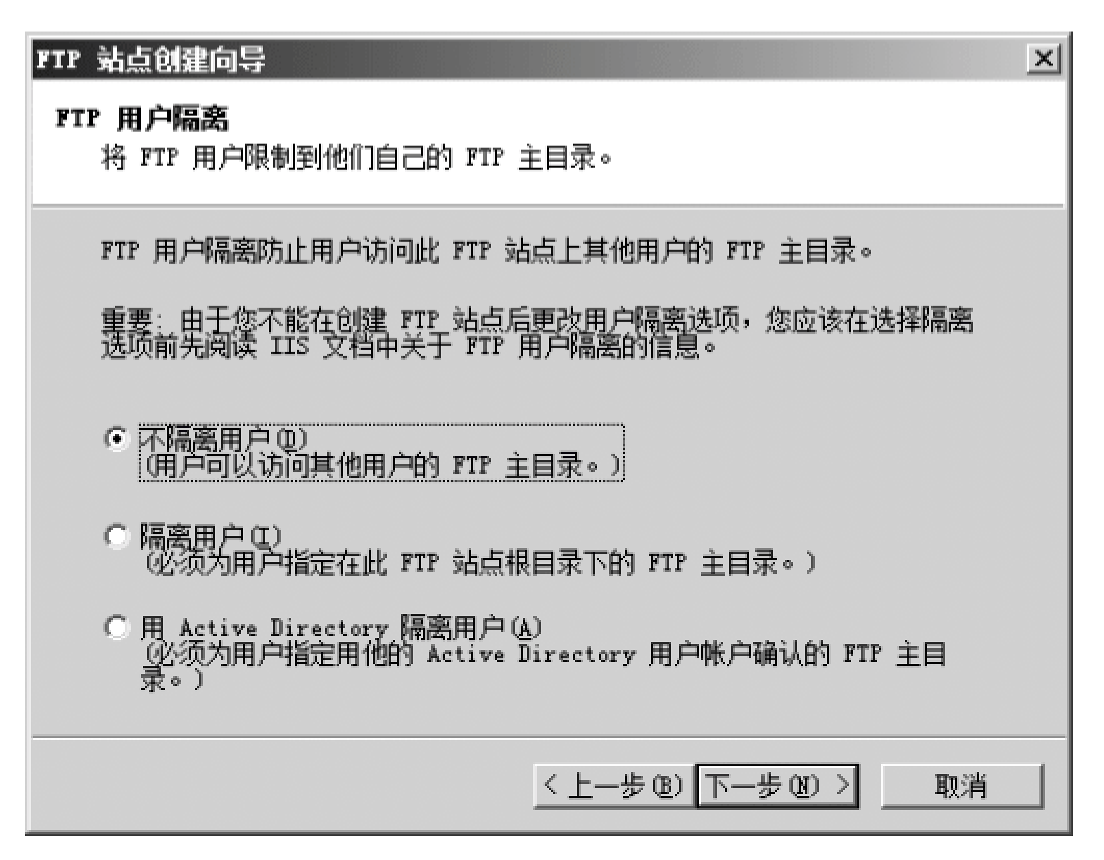


图 9-24　“FTP 用户隔离”界面

(5) 该界面有 3 个选项，各选项的含义分别如下。

- 不隔离用户：不启用 FTP 用户隔离，用户可以访问整个 FTP 站点，适用于只提供文件下载功能，或者不需要针对用户进行数据访问保护的 FTP 站点。
- 隔离用户：每个用户登录 FTP 时都需要验证，并限制在特定的主目录中，不允许浏览用户主目录外的内容，适用于为 Web 网站提供的维护服务，或者提供文件备份和存储服务的服务器。需要注意的是，如果创建的站点太多，则会影响服务器性能。
- 用 Active Directory 隔离用户：只能在域环境中应用，用户的主目录可放置在网络中的任意服务器上。该模式需要 Active Directory 服务器和文件服务器的支持，而且只能在局域网中使用。

根据需要选择合适的选项，选择完毕后，单击“下一步”按钮，进入“FTP 站点主目录”界面，如图 9-25 所示。

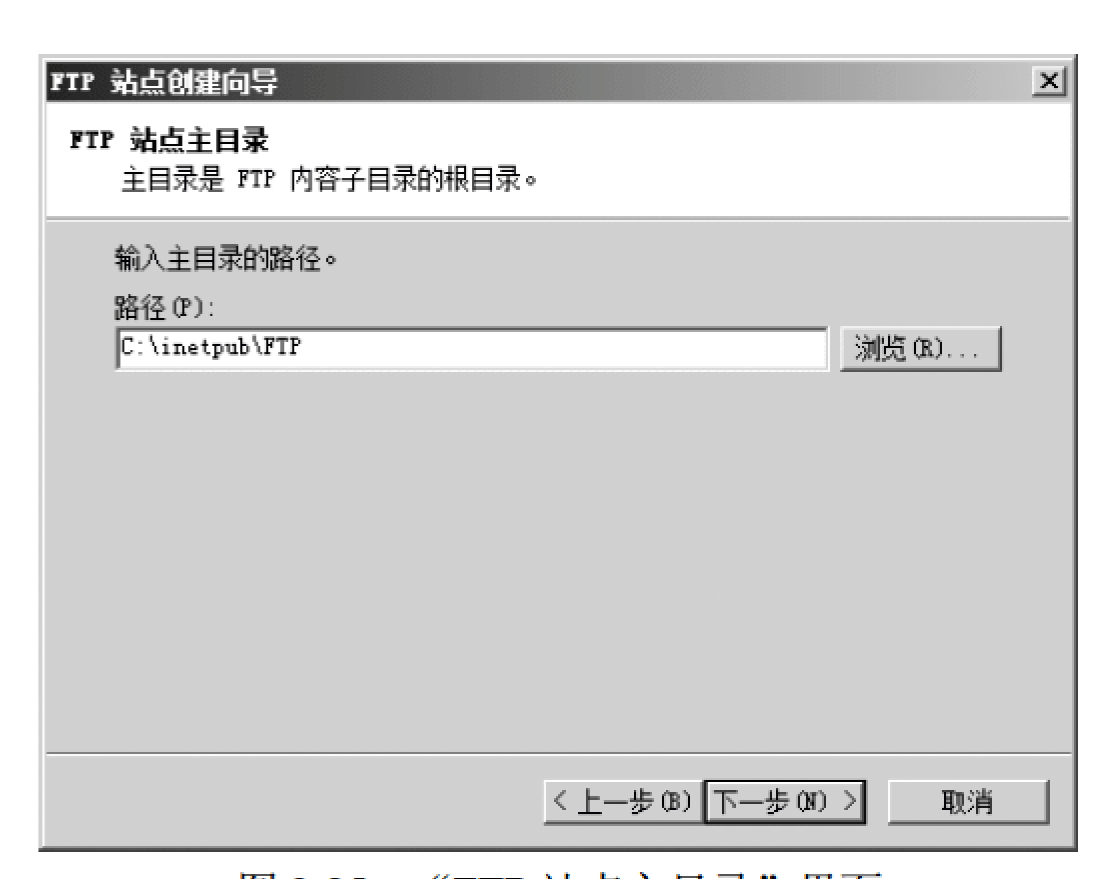


图 9-25　“FTP 站点主目录”界面

(6) 在“路径”文本框中输入当前 FTP 站点的主目录，然后单击“下一步”按钮，进入“FTP 站点访问权限”界面，如图 9-26 所示。

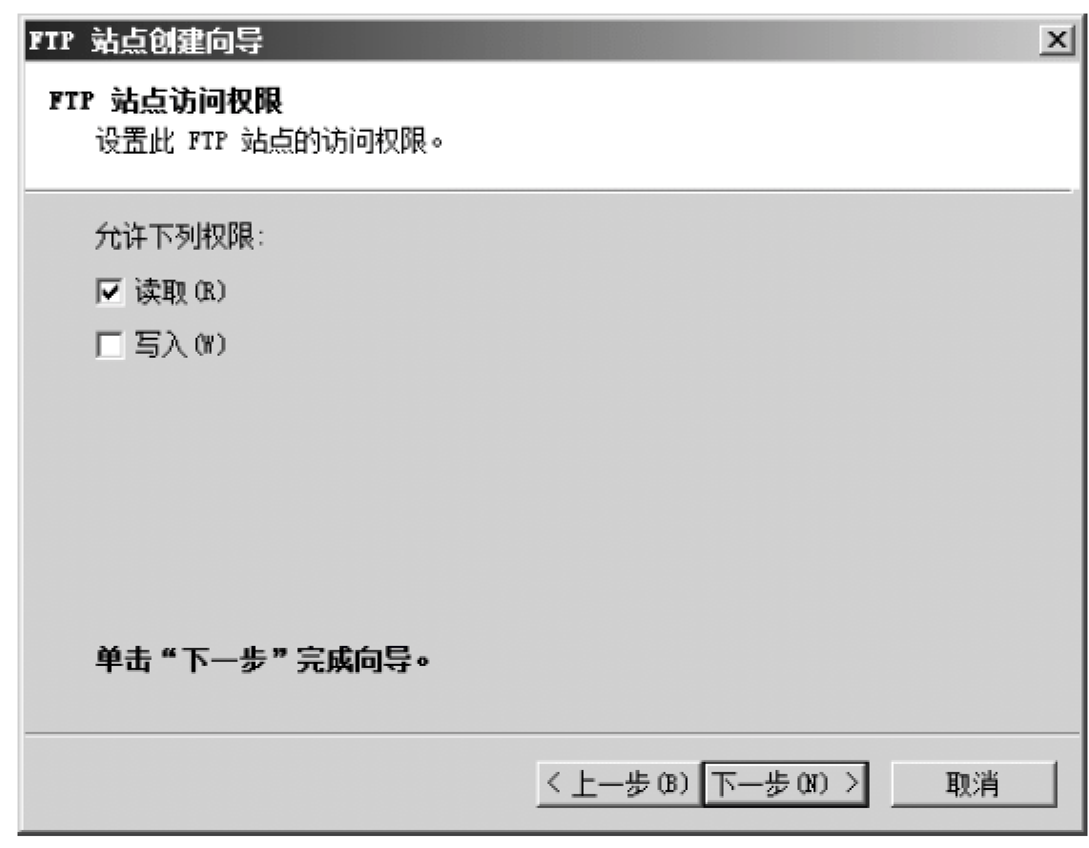


图 9-26　“FTP 站点访问权限”界面

(7) 设置好用户访问该 FTP 站点的权限，单击“下一步”按钮，进入站点建立完成界面，如图 9-27 所示。

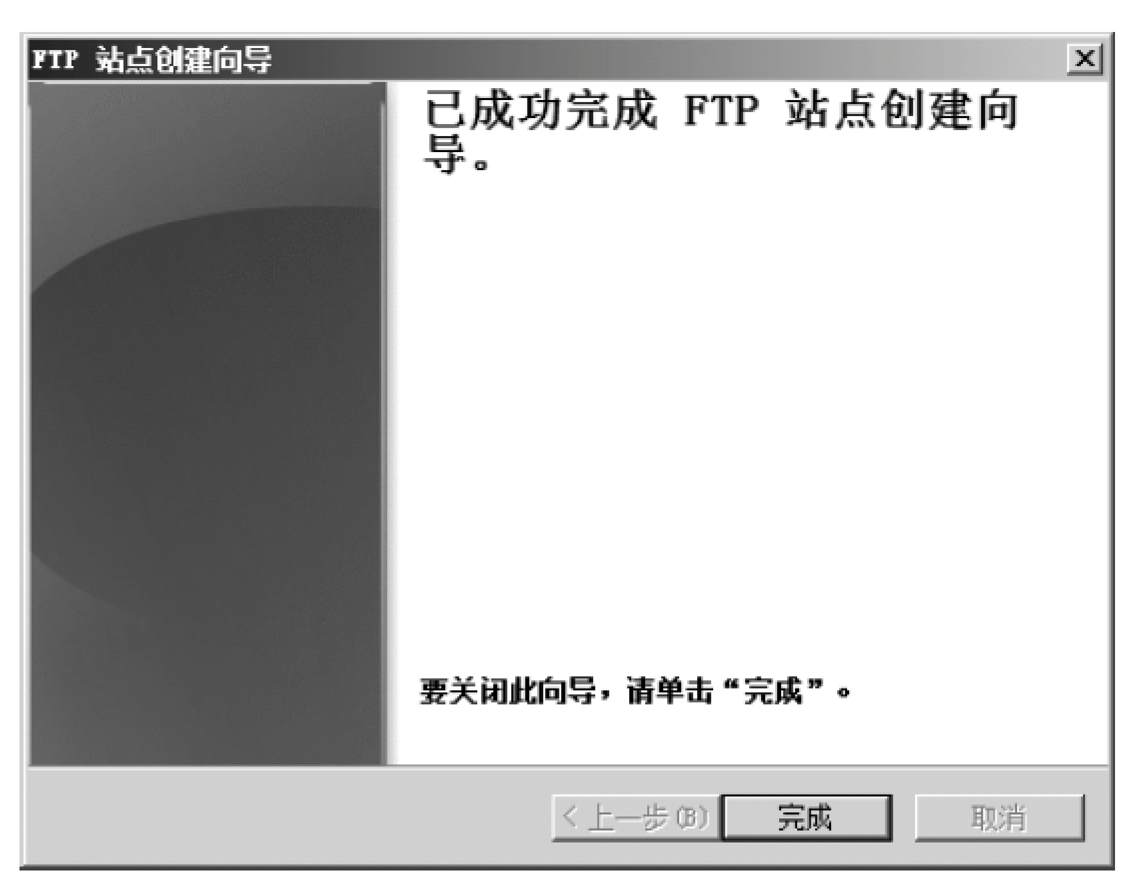


图 9-27　站点建立完成界面

(8) 单击“完成”按钮，关闭对话框，此时 IIS 管理器中出现新建好的站点，如图 9-28 所示。



图 9-28　IIS6.0 管理器界面

(9) FTP 虚拟站点的管理和默认 FTP 站点的管理方法完全相同，这里不再赘述。

9.3.2　虚拟目录

如果要扩展虚拟网站，为不同的用户提供不同的目录，他们还拥有不同的权限，此时不需要创建多个 FTP 站点，而应该利用虚拟目录来实现这个目的。使用虚拟目录可以创建多个不同内容，不同访问权限的目录，这些目录可能位于不同的卷，甚至网络中其他计算机的磁盘上，但是无论是管理还是使用都是在同一个 FTP 站点进行集中管理，非常方便。

FTP 虚拟目录是 FTP 站点的下一级目录。而且虚拟目录可以将处于不同位置的存储空间集中在同一个 FTP 站点中，便于访问和管理。

虚拟目录有以下特点。

- 便于扩展：当 FTP 站点升级或扩展时，如果需要扩展磁盘空间，而主目录所在卷空间不足，可以通过虚拟目录将其他卷或磁盘的空间添加到 FTP 站点中，用户使用时不会感到有任何差异。
- 增删灵活：可以根据需要随时向 FTP 站点增加或删除虚拟目录，而且在增加或删除过程中不会影响 FTP 站点的正常运行。
- 易于配置：虚拟目录是 FTP 站点的一个子目录，可以像访问 FTP 站点那样访问虚拟目录，即使一个 FTP 站点有多个虚拟目录，也一样通过 FTP 站点的 IP 地址和端口进行访问，就像访问一个目录下的多个子目录一样。此外，新建的虚拟目录自动继承 FTP 站点的权限，管理方便。

但是，虚拟目录不是一个独立的 FTP 站点，而是依附于一个 FTP 站点提供服务，这点要特别注意。

创建虚拟目录的操作方法如下：

(1) 打开 IIS 6.0 管理器，展开“FTP 站点”节点，右击想要创建虚拟目录的 FTP 站点，在弹出的快捷菜单中选择“新建”→“虚拟目录”命令，打开虚拟目录创建向导，如图 9-29 所示。

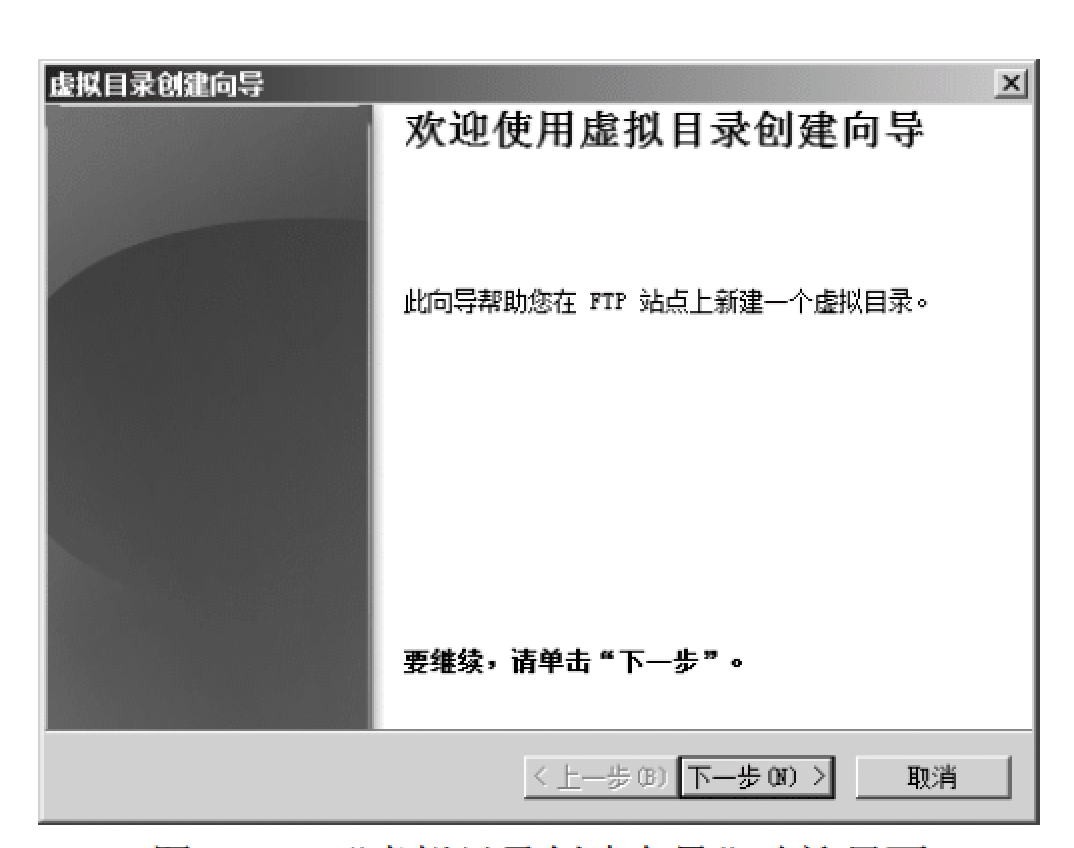


图 9-29　“虚拟目录创建向导”欢迎界面

(2) 单击“下一步”按钮，进入“虚拟目录别名”界面，如图 9-30 所示。

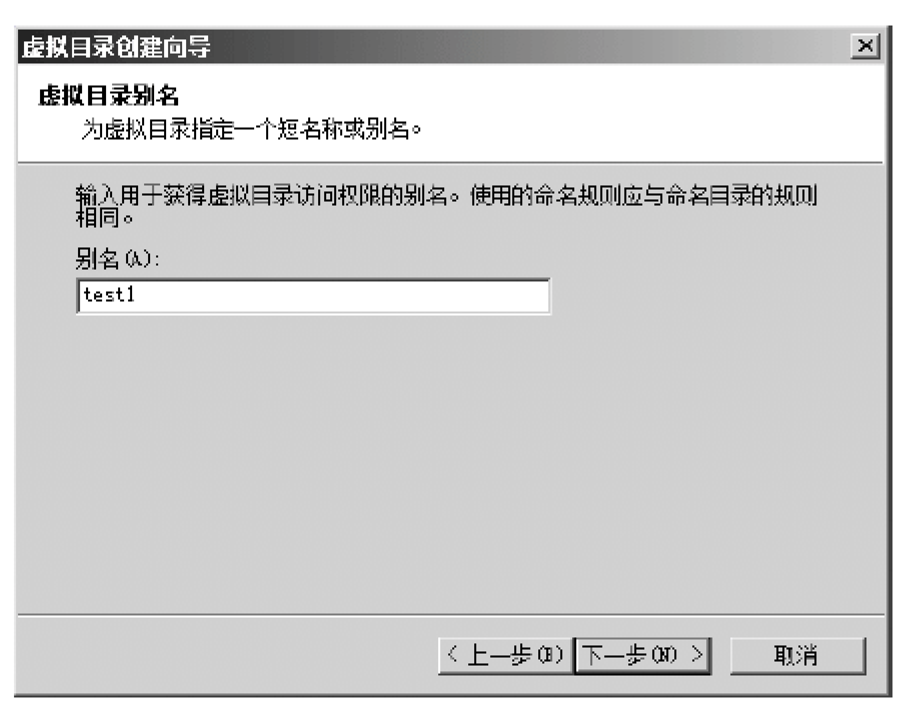


图 9-30　“虚拟目录别名”界面

(3) 在“别名”文本框中输入虚拟目录的别名，这个名字将在用户登录 FTP 站点后被看到，但这个别名和真实目录的名字没有关系。设置完毕后，单击“下一步”按钮，进入“FTP 站点内容目录”界面，如图 9-31 所示。

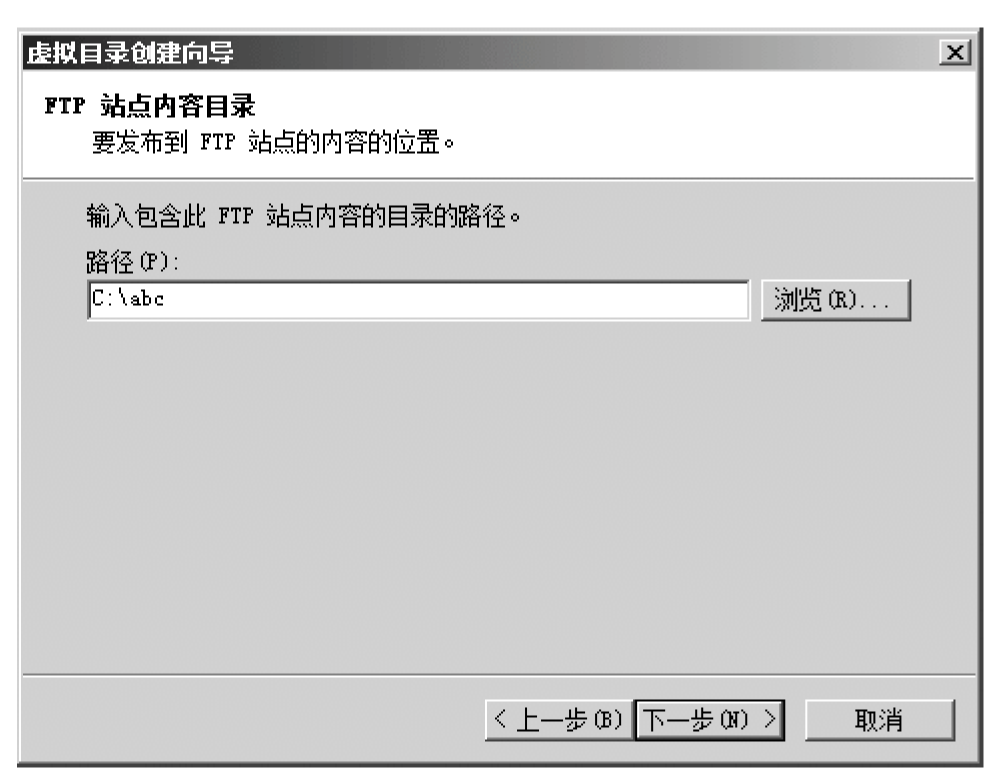


图 9-31　“FTP 站点内容目录”界面

(4) 在“路径”文本框中输入虚拟目录对应的真实目录所在的路径。将来用户访问虚拟目录时，实际上访问的就是本界面中输入的真实目录。设置完毕后，单击“下一步”按钮，进入“虚拟目录访问权限”界面，如图 9-32 所示。

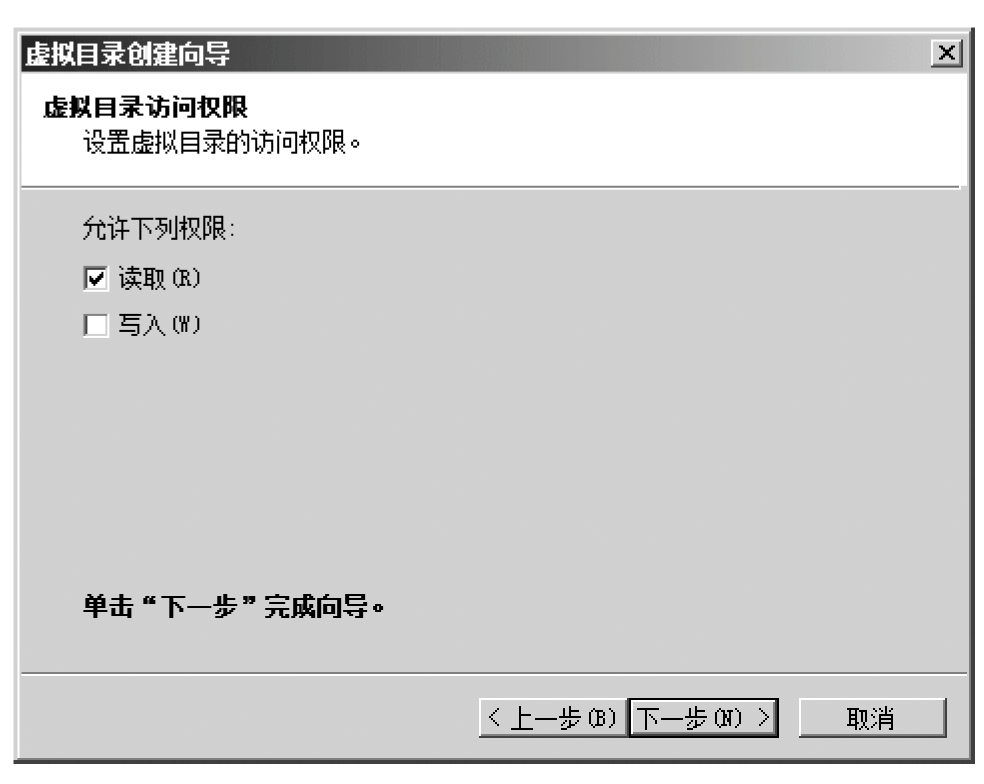


图 9-32　“虚拟目录访问权限”界面

(5) 在该界面设置对该虚拟目录的访问权限，然后单击“下一步”按钮，完成配置。

(6) 虚拟目录创建完毕后，就可以进行配置。在虚拟目录上右击，在弹出的快捷菜单中选择“属性”命令，打开“属性”对话框，如图 9-33 所示。



图 9-33　“属性”对话框

(7) 在该界面中可以设置虚拟目录对应的真实目录的路径，以及用户访问该虚拟目录时拥有的权限。

9.4　FTP 站点的访问安全

如果 FTP 站点中存放的是较重要的文件，那么，FTP 站点的安全就是一个比较重要的问题。管理员可以通过限制来访帐户和来访计算机来加强 FTP 站点的安全性。

9.4.1　禁止匿名访问

在默认设置下，IIS 中的 FTP 服务是允许匿名访问的，即用户无需输入用户名和密码就可以访问 FTP 站点的文件和文件夹。如果 FTP 站点存放的是比较重要的文件，应当禁止匿名用户访问，只对指定的用户开放。

首先，打开 IIS 6.0 管理器，打开要进行配置的 FTP 站点的属性对话框，打开“安全帐户”选项卡，如图 9-34 所示。

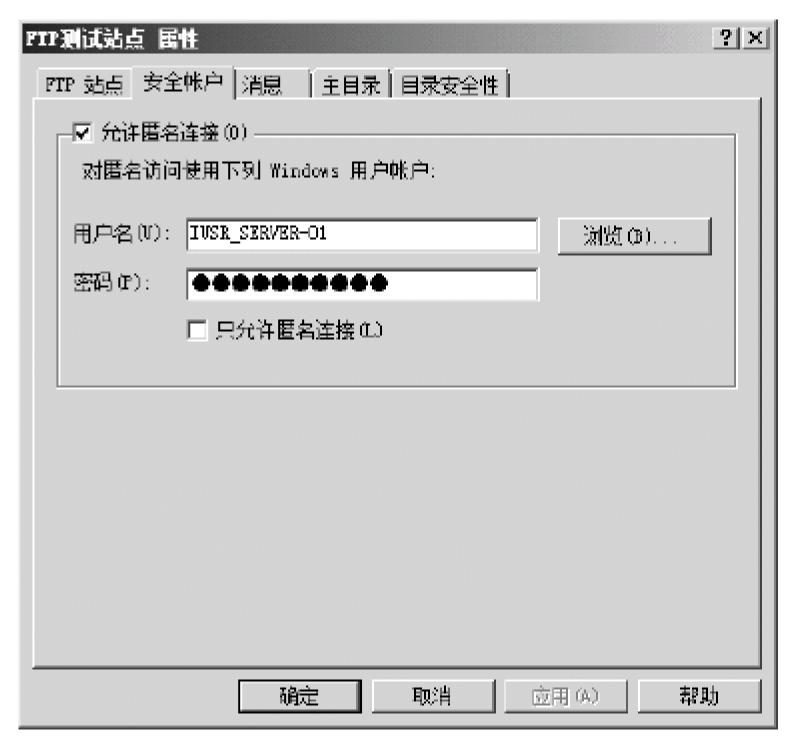


图 9-34　“安全帐户”选项卡

如果选中“只允许匿名连接”复选框，则不允许任何用户使用指定的帐户进行登录，只能实现匿名登录。在对安全性要求较高的 FTP 站点中，是不允许的。如果要取消匿名登录，应当取消选中“允许匿名连接”复选框，然后单击“确定”按钮。这样 FTP 站点将不允许匿名登录，用户登录 FTP 站点时必须输入用户名和密码。

取消 FTP 站点的匿名登录后，再通过计算机管理器为系统添加一个用户，然后在 FTP 站点主目录的 NTFS 权限设置中添加该用户，并根据需要为其分配权限，这样就可以使用该用户的用户名和密码登录 FTP 服务器了。

9.4.2　限制 IP 地址访问

除了限制登录用户以外，还可以只允许(或禁止)指定 IP 地址的计算机访问 FTP 站点，以提高安全性。允许信任的 IP 地址访问 FTP 站点，禁止不信任的 IP 地址访问 FTP 站点，这样不被信任的 IP 地址将不能访问 FTP 站点，避免了来自外界的攻击，大大提高了 FTP 站点的安全性。即使 FTP 站点被攻击，也可以根据受信任的 IP 地址列表，缩小查找范围，有利于查清问题发生的原因。这种设置方式在企业网络中比较常用。

具体操作步骤如下：

(1) 打开要进行配置的 FTP 站点的属性对话框，打开其中的“目录安全性”选项卡，如图 9-35 所示。



图 9-35　“目录安全性”选项卡

(2) “目录安全性”选项卡中一共有两个选项。如果选中“授权访问”，则允许所有的计算机都可以访问 FTP 站点，但是指定的 IP 地址除外，也就是指定拒绝访问该 FTP 站点的 IP 地址是哪些；如果选中“拒绝访问”，则禁止所有的计算机访问 FTP 站点，但是指定的 IP 地址除外，也就是指定允许访问该 FTP 站点的 IP 地址有哪些。选择好策略后，单击“添加”按钮，打开添加 IP 地址对话框，如图 9-36 所示。



图 9-36　“拒绝访问”对话框

(3) 默认状态下是选中“一台计算机”单选按钮，在“IP 地址”文本框中输入指定的 IP 地址，单击“确定”按钮完成配置。这种方法可以添加单个 IP 地址。还可以选中“一组计算机”单选按钮，如图 9-37 所示。



图 9-37　“拒绝访问”对话框

(4) 在“网络标识”文本框中输入网络号，在“子网掩码”文本框中输入子网掩码，就可以添加一个网段的 IP 地址了。单击“确定”按钮完成配置。

9.5　FTP 站点的访问

FTP 站点设置成功后，就可以为用户提供服务了。根据 FTP 站点的权限设置的不同，用户对 FTP 站点可进行的操作也有所不同。一般来说，访问 FTP 站点有两种方式，一是 Windows 资源管理器，二是专用 FTP 软件。

9.5.1　访问 FTP 站点

如果使用 Windows 资源管理器访问 FTP 站点，首先打开 Windows 资源管理器，然后在地址栏中输入 FTP 站点的地址，按下回车键，开始登录 FTP 站点。FTP 站点的地址格式是 ftp://服务器名或 IP 地址/目录名称：端口号，如果 FTP 站点的端口号是默认的 21，则不需要输入端口号和它前面的冒号。例如，一个 FTP 站点的 IP 地址是 192.168.5.2，端口号是 20(注意，不是默认的 21 端口)，登录该站点时，它的地址是“ftp://192.168.5.2:20”(不含引号)。

如果该 FTP 站点允许匿名登录，用户会直接以匿名用户身份登录该 FTP 站点。如果 FTP 站点不允许匿名登录，则会弹出“登录身份”对话框，如图 9-38 所示。

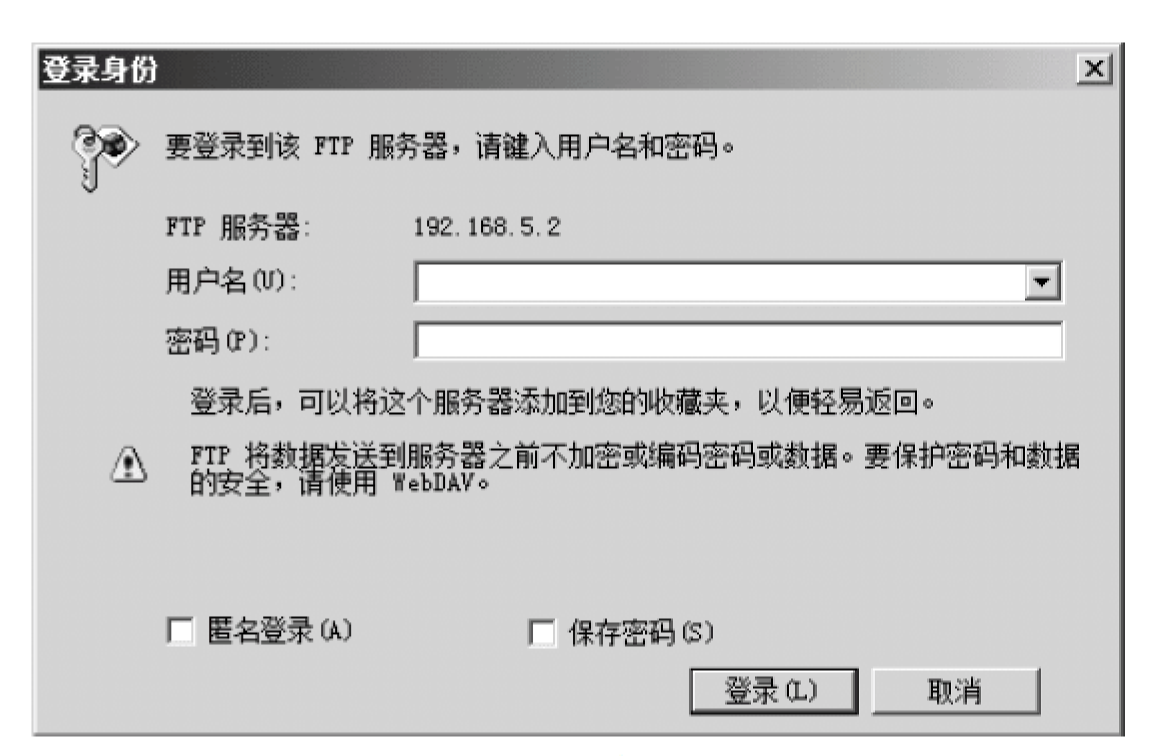


图 9-38　“登录身份”对话框

输入登录用户的用户名和密码，单击“登录”按钮，如果用户名和密码正确，就会登录到服务器上。

如果 FTP 服务器既允许匿名登录，也允许通过用户名登录，那么登录时 Windows 资源管理器自动以匿名用户身份登录到服务器。此时如果还想以指定帐户登录，可以在页面空白处右击，在弹出的快捷菜单中选择“登录”命令，就会打开如图 9-38 所示的“登录身份”对话框，输入用户名和密码即可。

通过 Windows 资源管理器登录 FTP 站点以后，上传和下载操作的方法和在两个文件夹中复制和粘贴文件是一样的。如果想下载文件，在选定文件上右击，在弹出的快捷菜单中选择“复制”命令，再打开想要保存文件的文件夹，在空白处右击，在弹出的快捷菜单中选择“粘贴”命令；如果想上传文件，在要上传的本地文件上右击，在弹出的快捷菜单中选择“复制”命令，再在打开的 FTP 站点的页面空白处右击，在弹出的快捷菜单中选择“粘贴”命令。但是具体可以进行的操作取决于 FTP 站点对权限的设置。

如果使用专用 FTP 软件登录，虽然设置会稍有麻烦，但是使用更加便利，效率更高。下面以 CuteFTP 为例，介绍具体的操作方法。

首先运行 CuteFTP 程序，依次选择“文件”菜单→“新建”→“FTP 站点”命令，打开“站点属性”对话框，如图 9-39 所示。

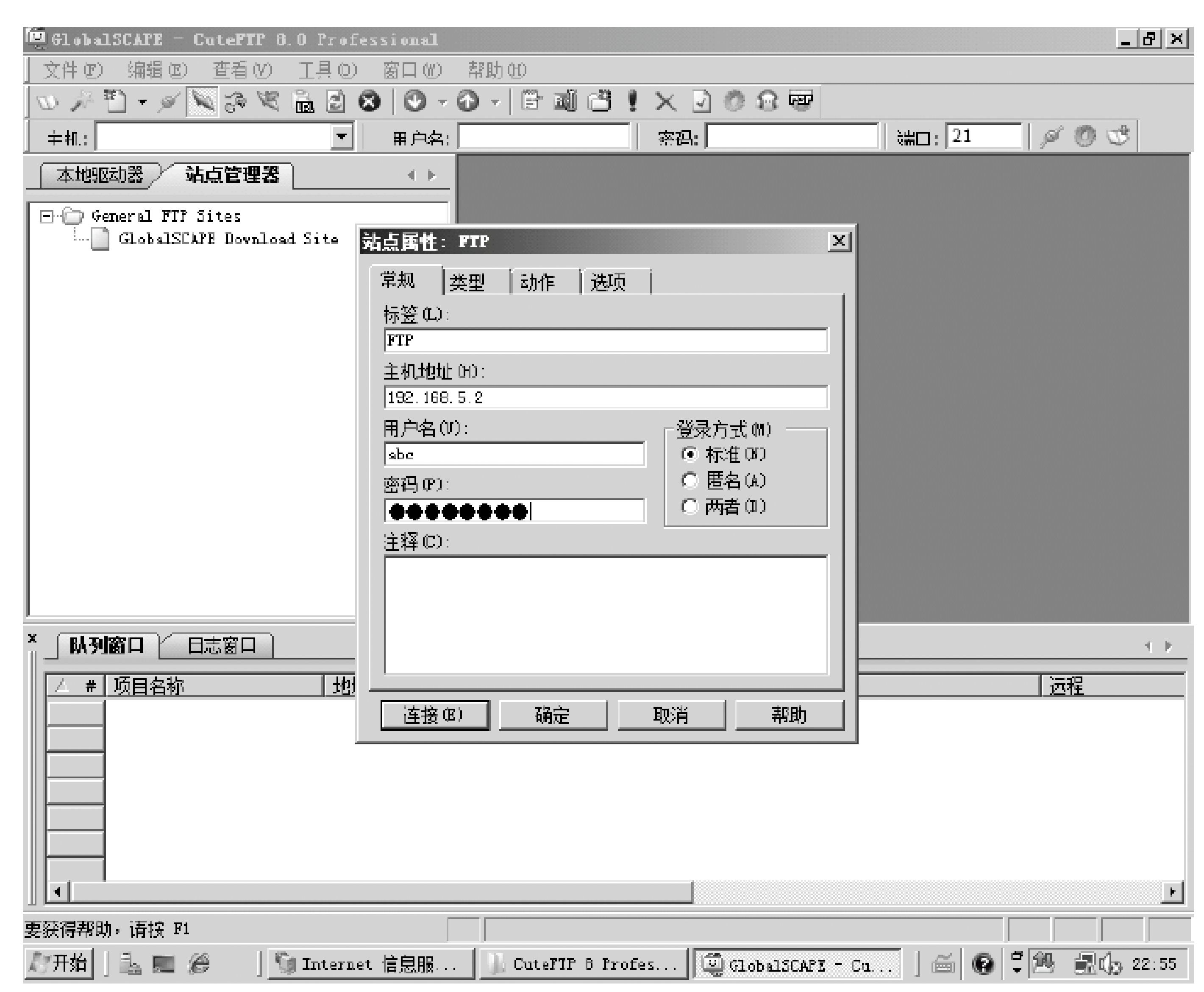


图 9-39　“站点属性”对话框

设置各项信息，在“标签”文本框输入 FTP 站点名称，“主机地址”文本框输入 FTP 站点地址；登录方式如果选择“匿名”，则不需要输入用户名和密码两项信息，如果选择“标准”或者“两者”，则需要输入用户名和密码。如果 FTP 站点的端口号不是默认的 21 端口，还需要打开“类型”选项卡修改该站点的访问端口。

设置完毕，单击“连接”按钮，即可自动连接 FTP 站点，如图 9-40 所示。

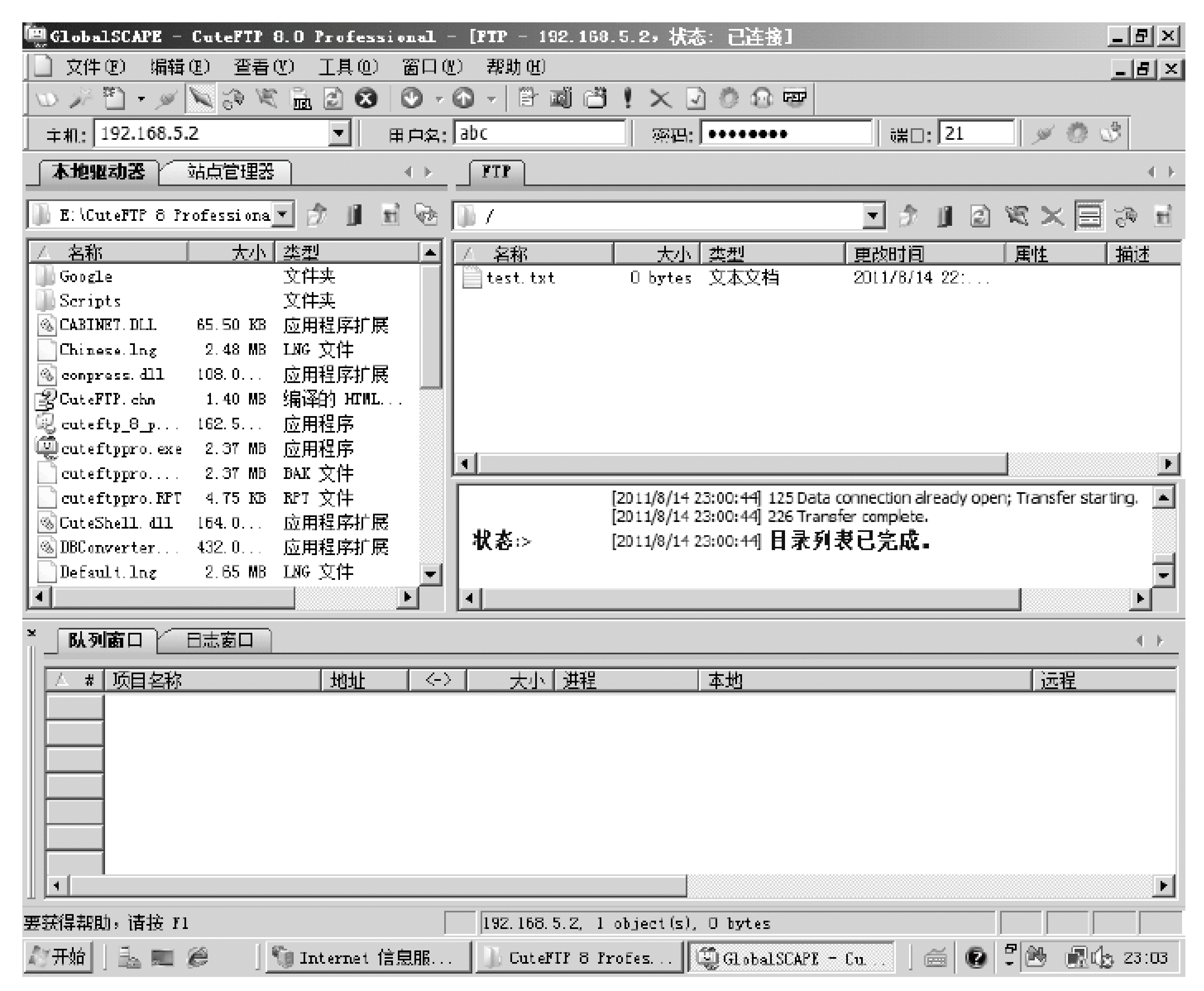


图 9-40　CuteFTP 界面

CuteFTP 的界面可以分为四大部分，上方是软件的菜单栏和工具栏，下方是文件传输的状态栏，中间分为左右两个窗格，左侧窗格为本地驱动器栏，显示本地资源，右侧窗格为 FTP 站点栏，显示 FTP 站点上的资源。如果要进行下载操作，从右侧窗格将要下载的文件或文件夹拖到左侧窗格即可，如果要进行上传操作，将要上传的文件或文件夹从左侧窗格拖到右侧窗格即可。

9.5.2　虚拟目录的访问

通过上述方法登录到 FTP 站点后，虚拟目录并不会直接显示出来。如果要访问虚拟目录，可以在登录时，在FTP站点地址中加上目录的路径。如FTP站点的IP地址为192.168.5.2，其中有一个虚拟目录名为 test1，端口号为 21，如果要访问 test1 目录，则访问地址是 ftp://192.168.5.2/test1。

其他方面和访问 FTP 站点相同，这里不再赘述。

9.6　本章小结

本章介绍了使用 IIS 搭建 FTP 服务器的方法，通过 IIS，用户可以搭建安全、高效的 FTP 服务器，也可以利用一台服务器，搭建多个 FTP 服务器，提高了硬件的使用效率，降低了开销。用户则可以根据情况使用不同的方法和工具使用 FTP 服务。

(1) FTP 服务器的搭建与配置：本节介绍了在 IIS 中启用 FTP 服务的方法，通过学习，学生可以利用 IIS 6 搭建 FTP 服务器，设置 FTP 服务器参数和提示信息。

(2) 为 FTP 设置 NTFS 访问权限：本节介绍了 FTP 服务器权限设置的方法，通过学习，学生可以设定用户对 FTP 服务器的访问权限，如果 FTP 主目录位于 NTFS 卷上，还可以将两者配合起来，实现更加灵活细致的权限分配。

(3) 虚拟站点与虚拟目录：本节介绍了创建虚拟目录和虚拟站点的方法，通过学习，学生可以在同一台服务器上创建多个目录和站点，提高服务器硬件的使用效率，节约了开销。

(4) FTP 站点的访问安全：本节介绍了针对 FTP 站点的安全设置，主要包括指定可访问服务器的帐户和限制可访问服务器的 IP 地址两个方法。

(5) FTP 站点的访问：本节介绍了访问 FTP 站点的方法，可以使用 Windows 资源管理器实现简单访问，也可以使用更加专业的 FTP 工具进行访问。访问普通 FTP 站点和虚拟站点、虚拟目录的方法是一样的。

9.7　思考与练习

【思考题】

1. 如果服务器允许匿名登录，是否用户可以不需要任何账户即可享用 FTP 服务？
2. 说明 FTP 服务器权限设置和 NTFS 权限设置之间的关系。

【练习题】

1. 配置 FTP 服务的基本参数(参考 9.1.2 节)、磁盘配额(参考 9.2.3 节)并发布。
2. 限制只有某个 IP 地址段可访问 FTP 服务器(参考 9.4.2 节)。

第10章　邮件服务

【本章导读】

Exchange Server 2007 不仅具有邮件服务器的功能，而且是一款功能强大的企业信息平台。本章主要介绍 Exchange Server 2007 与邮件服务器有关的最基本的功能，内容包括 Exchange Server 2007 概述、安装 Exchange Server 2007、使用 Exchange 管理控制台建立用户邮箱、客户端的使用、配置面向 Internet 的集线器传输服务器、邮箱常用操作和限制，通过本章的学习，可构建一个简单的邮件系统，并在客户端使用 OWA 或 Outlook 2007 进行邮件收发。

10.1　Exchange Server 概述

10.1.1　邮件系统概述

电子邮件是最基本的网络通信功能之一。电子邮件的传输是通过电子邮件简单传输协议(Simple Mail Transfer Protocol，SMTP)这一系统软件来完成的。电子邮件系统的重要组成部分是邮件服务器。从硬件上看，邮件服务器是一台高性能、大容量的计算机。硬盘作为邮箱的存储介质，在硬盘上为用户分配一定的存储空间作为用户的邮箱，不同用户的邮箱可能存在于同一个邮件服务器上，也可能存在于不同的邮件服务器上。客户端发送邮件时，先把邮件发送给自己的邮件服务器，邮件服务器根据收件人的邮箱地址确定收件人邮箱所在的邮件服务器，然后把邮件发送过去，收件人所在的邮件服务器再把邮件放入收件人的邮箱。收件人客户端连接自己的邮件服务器就能收到发给自己的邮件了。

邮件服务器是需要软件支持的，这样的软件有多种。主要有：(1)基于 Postfix/Qmail 的邮件系统；(2)微软的 Exchange 邮件系统；(3)IBM Lotus Domino 邮件系统；(4)Scalix 邮件系统；(5)Zimbra 邮件系统；(6)MDeamon 邮件系统。其中，Exchange 邮件系统由于和 Windows 整合，便于管理，是在企业中使用数量最多的邮件系统；IBM Lotus Domino 则综合功能较强，大型企业使用较多；基于 Postfix 的邮件系统则需要有较强的技术力量才能实现，但是性能可以达到非常高，而且安全性很好。

Exchange 2007 在架构上采用 64 位硬件平台(也提供 32 位的测试版本)，简化了管理机制和路由选择。主要的变化是服务器以角色为基础的部署，服务器的角色共分为五类：边缘传输、集线器传输、客户端访问、统一消息和邮箱。

1. 边缘传输(Edge Transport)

"边缘传输"服务器角色以独立服务器的形式存在于内部网络之外，通常用防火墙进行隔离。它可使内部网络受到外部攻击的机率减到最小，如没有构建边缘传输服务器，则"集线器传输"服务器将直接面对外部网络进行邮件收发，这就降低了内部网络的安全性。

边缘传输服务器可以接收来自 Internet 的邮件，经处理后，发送到企业内部的集线器传输服务器。企业内部发送到 Internet 的邮件也要通过集线器传输服务器传送到边缘传输服务器，经处理后发送到 Internet。

边缘传输服务器提供多层次的垃圾邮件筛选与保护程序，能够准确地过滤垃圾邮件，同时使用边缘传输规则，有效地保护企业网络资源。

2. 集线器传输(Hub Transport)

集线器传输服务器部署在 Active Directory 域内部，用于处理组织内的所有邮件流、应用传输规则、应用日记策略以及向收件人的邮箱传递邮件。发送到 Internet 的邮件由集线器传输服务器传输到边缘传输服务器，再发送到 Internet。从 Internet 接收的邮件在传输到集线器传输服务器之前，由边缘传输服务器进行处理。如果不具有边缘传输服务器，则可以将集线器传输服务器进行配置，使之直接中继 Internet 邮件。还可以在集线器传输服务器上安装和配置边缘传输服务器代理程序，用来在组织内部提供反垃圾邮件和防病毒保护的服务。

集线器传输服务器将其所有配置信息都存储在 Active Directory 中。这些信息包括传输规则、日记规则和连接器配置。由于这些信息存储在 Active Directory 中，因此组织中的每个集线器传输服务器都可应用这些相同的设置。

集线器传输服务器角色可与其他任何非群集内部服务器角色安装在同一服务器上，或者安装在集线器传输服务器角色专用的服务器上。每个包含邮箱服务器角色的 Active Directory 站点中必须部署集线器传输服务器。每个站点中可部署多个集线器传输服务器，这会将连接请求分散处理，同时在其中一台服务器出故障时提供容错能力，以免服务中断。

3. 客户端访问(Client Access)

客户端访问服务器具有处理来自 Internet 客户端请求的能力，并依据负载平衡原则，将接收的流量发送到后端适当的服务器中。

客户端访问服务器支持 Microsoft Outlook Web Access(OWA)和 Microsoft Exchange ActiveSync 客户端应用程序以及邮局协议第 3 版(POP3)和 Internet 信息访问协议第 4 版(IMAP4)。客户端访问服务器还支持一些服务，例如 Autodiscover 服务和 Web 服务。

使用上述方法，客户端都可以连接到客户端访问服务器。例如，Microsoft Outlook Express 使用 POP3 或 IMAP4 与 Exchange 服务器通信，而手机或 PDA 则使用 ActiveSync、POP3 或 IMAP4 与 Exchange 服务器通信。

4. 统一消息(Unified Message，UM)

统一消息服务器提供了整合 PBX(Private Branch eXchange)的电话信息交换能力，允许用户通过任何电话访问其 Exchange 2007 邮箱中的电子邮件、语音邮箱、传真信息与联系人信息等。

5. 邮箱

邮箱服务器负责将客户端邮箱的内容存储在数据库中，并且允许进行复制或群集结构等可用性规划。除此之外，它还负责控制公用文件夹，并且产生离线通讯簿。

每台邮箱服务器必须与以下的组件协同工作：

- Active Directory 目录服务服务器
- 集线器传输服务器
- 客户端访问服务器
- 统一消息服务器
- Microsoft Outlook 客户端

10.1.2　系统安装需求

1. CPU 需求

32 位试用版：Intel Pentium 800(MHz)或更高等级处理器。

64 位版本：x64 架构计算机且支持 Intel Extended Memory 64 技术(Intel EM64T)的 Intel Xeon 或 Intel Pentium 系列处理器，或支持 AMD64 平台的 AMD Opteron 或 AMD Athlon 64 处理器。

不支持的 CPU 类型：Intel Itanium IA64。

2. 操作系统需求

Windows Server 2003 各版本、Windows Server 2008 标准版、Windows Server 2008 企业版。

3. 内存需求

至少 2GB 内存，建议的内存数量为 2GB 和每用户 2MB~5MB。

4. 硬盘空间需求

至少 1.2GB 的硬盘空间，若要为“统一消息”安装其他语言插件，每种语言需要额外的 500MB 的硬盘空间。在使用“本机连续复制”或“群集连续复制”时需额外空间，而实际需求量则按照要复制的存储组大小而定。

5. 媒体访问需求

DVD/光驱、本机硬盘、网络访问。

6. 文件格式需求

格式化为 NTFS 文件系统的磁盘分区。

7. 软件需求

- Microsoft .NET Framework Version 2.0
- Microsoft Management Console(MMC) 3.0
- Windows PowerShell

10.2　安装 Exchange Server

10.2.1　准备工作

Exchange Server 既可以安装在成员服务器上，也可以安装在域控制器上，在此将其安装在域控制器上。在安装 Exchange Server 2007 之前需要添加 Web 服务和 Windows PowerShell，这些工作需要以 Administrator 的身份登录域之后才能进行(如无特别声明，软件安装过程中所做的操作都是在以 Administrator 的身份登录域之后进行的)，首先添加 Web 服务。

(1) 依次选择“开始”→“管理工具”→“服务器管理器”，在“服务器管理器”窗口中单击“角色”，然后单击右侧窗格中的“添加角色”，如图 10-1 所示。



图 10-1　选择“添加角色”

(2) 在出现的“开始之前”对话框中单击“下一步”按钮。

(3) 如图 10-2 所示，在“选择服务器角色”对话框中选中“Web 服务器(IIS)”复选框。并在弹出的对话框中单击“添加必需的功能”按钮，如图 10-3 所示。



图 10-2　选中“Web 服务器(IIS)”复选框

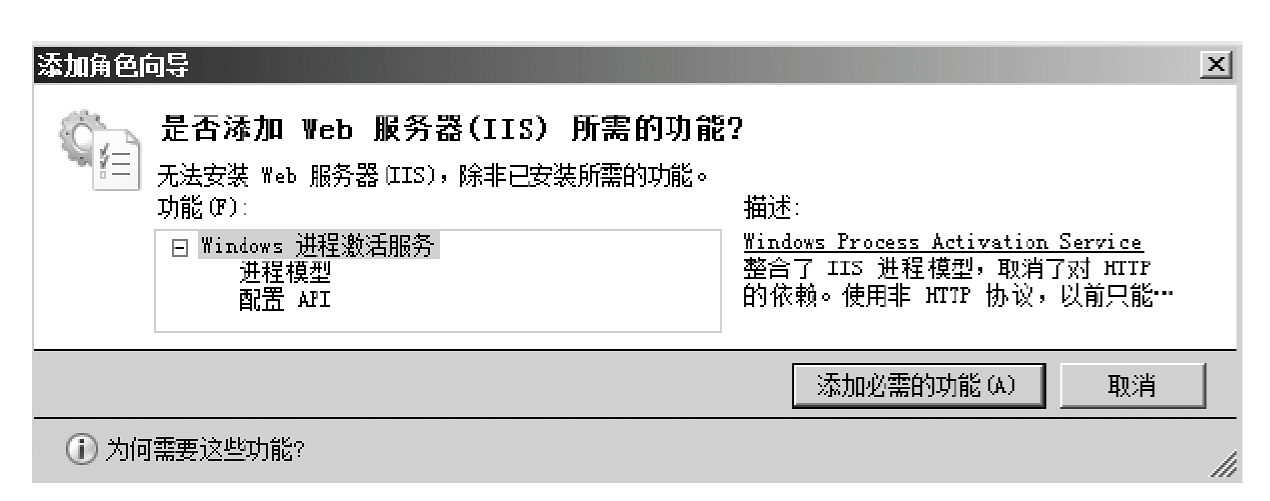


图 10-3　单击“添加必须的功能”

(4) 在出现的“Web 服务器(IIS)”对话框中单击“下一步”按钮。

(5) 在“选择角色服务”界面中，除了默认选中的项目外，还要选中“ASP.NET”、“静态压缩”、“动态压缩”、“身份验证服务”、“IIS6.0 管理兼容性”、“IIS 管理控制台”这些项目，然后单击“下一步”按钮，如图 10-4 所示。

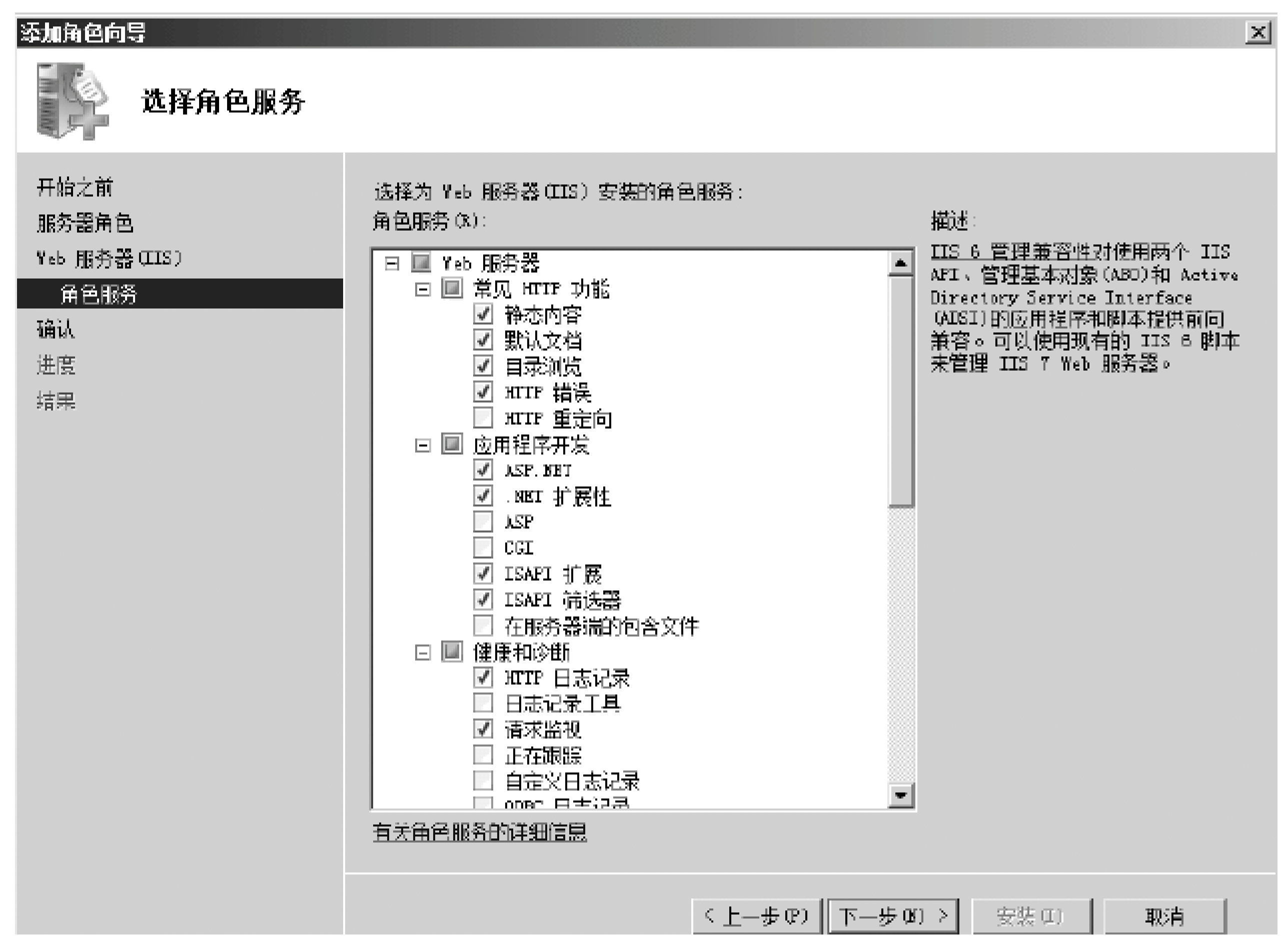


图 10-4　选中必要的项目

(6) 在出现的“确认安装选择”对话框中单击“安装”按钮，然后进入“安装进度”对话框，等待安装结束。

(7) 安装结束后，弹出“安装结果”对话框，单击“关闭”按钮，结束添加 Web 服务器。

接下来添加 Windows PowerShell，操作步骤如下：

(1) 在“服务器管理器”窗口中选择“功能”选项，然后单击右侧窗格中的“添加功能”，如图 10-5 所示。



图 10-5　单击“添加功能”

(2) 在出现的“选择功能”对话框中，选中“Windows PowerShell”，然后单击“下一步”按钮。

(3) 在出现的“确认安装选择”对话框中单击“安装”按钮，然后弹出“安装进度”对话框，最后出现“安装结果”对话框，在此对话框中单击“关闭”按钮。

到此就完成了添加 Web 服务和 Windows PowerShell 的操作。

10.2.2　安装 Exchange Server

在此安装 Exchange Server 2007 SP1 的 32 位试用版，可以从微软网站上下载安装程序。下载的是一个自解压的压缩包。可以把安装程序解压到硬盘的一个文件夹中，如图 10-6 所示，安装程序被解压到 E:\exchangesetup 文件夹中。

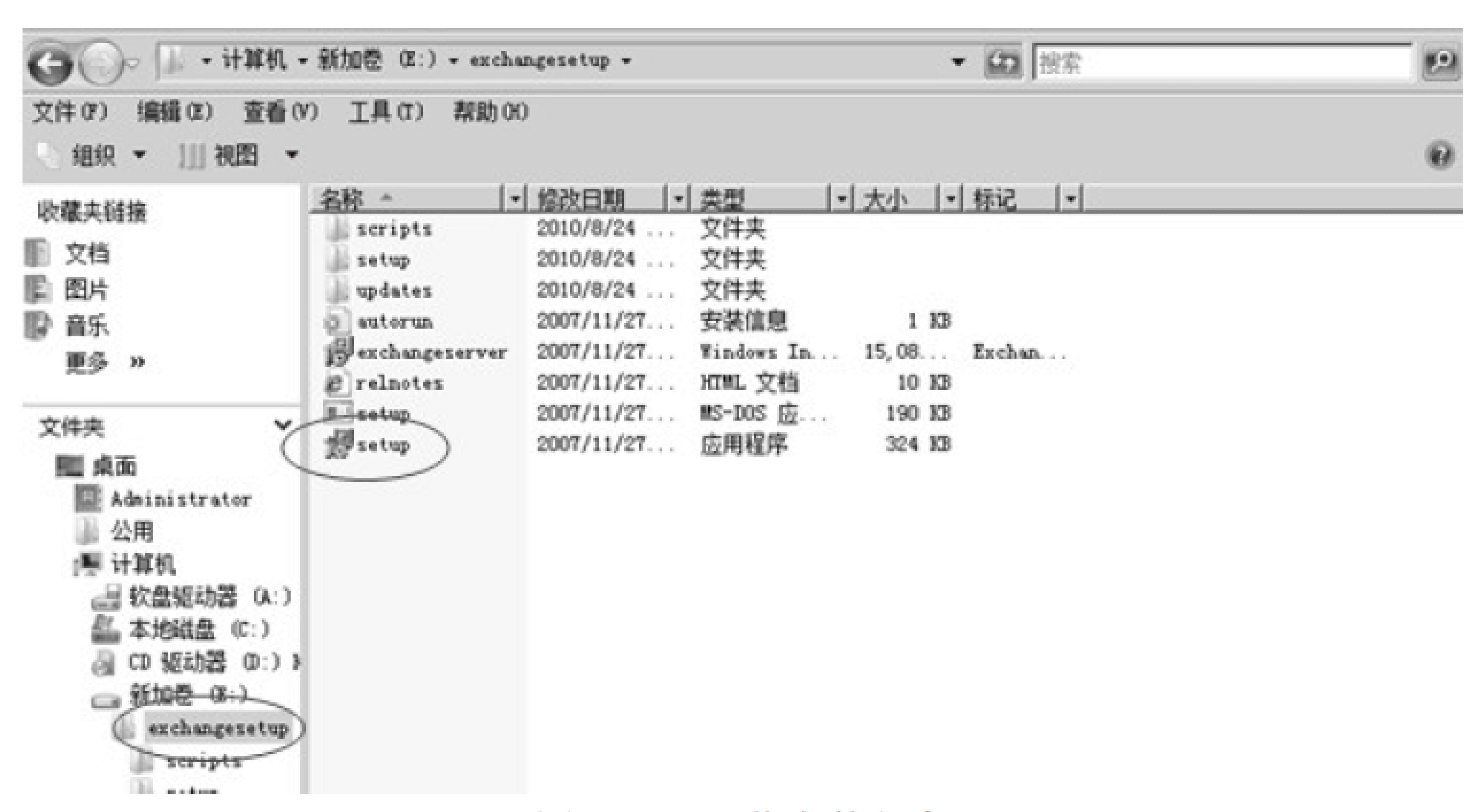


图 10-6　下载安装程序

安装步骤如下：

(1) 双击该文件夹下的 setup.exe 程序，就可以启动 Exchange Server 2007 的安装程序。

(2) 安装的前 3 个步骤呈灰色，如图 10-7 所示，是因为 NET Framework 2.0 和 Microsoft 管理控制台(MMC)包含在 Windows Server 2008 系统中，而 Microsoft Windows PowerShell 又在准备阶段进行了添加，因此可以直接从第 4 个步骤开始安装。选择步骤 4 后，在弹出的对话框中单击“下一步”按钮。



图 10-7　安装 Exchange Sever 2007

(3) 在如图 10-8 所示的“许可协议”界面中，选中“我接受许可协议中的条款”单选按钮，单击“下一步”按钮，如图 10-8 所示。



图 10-8　查看许可协议

(4) 在显示的“错误报告”界面中，询问是否愿意启用错误报告的功能，即系统出现错误时，是否自动向微软公司传送报告，选择后单击“下一步”按钮，如图 10-9 所示。

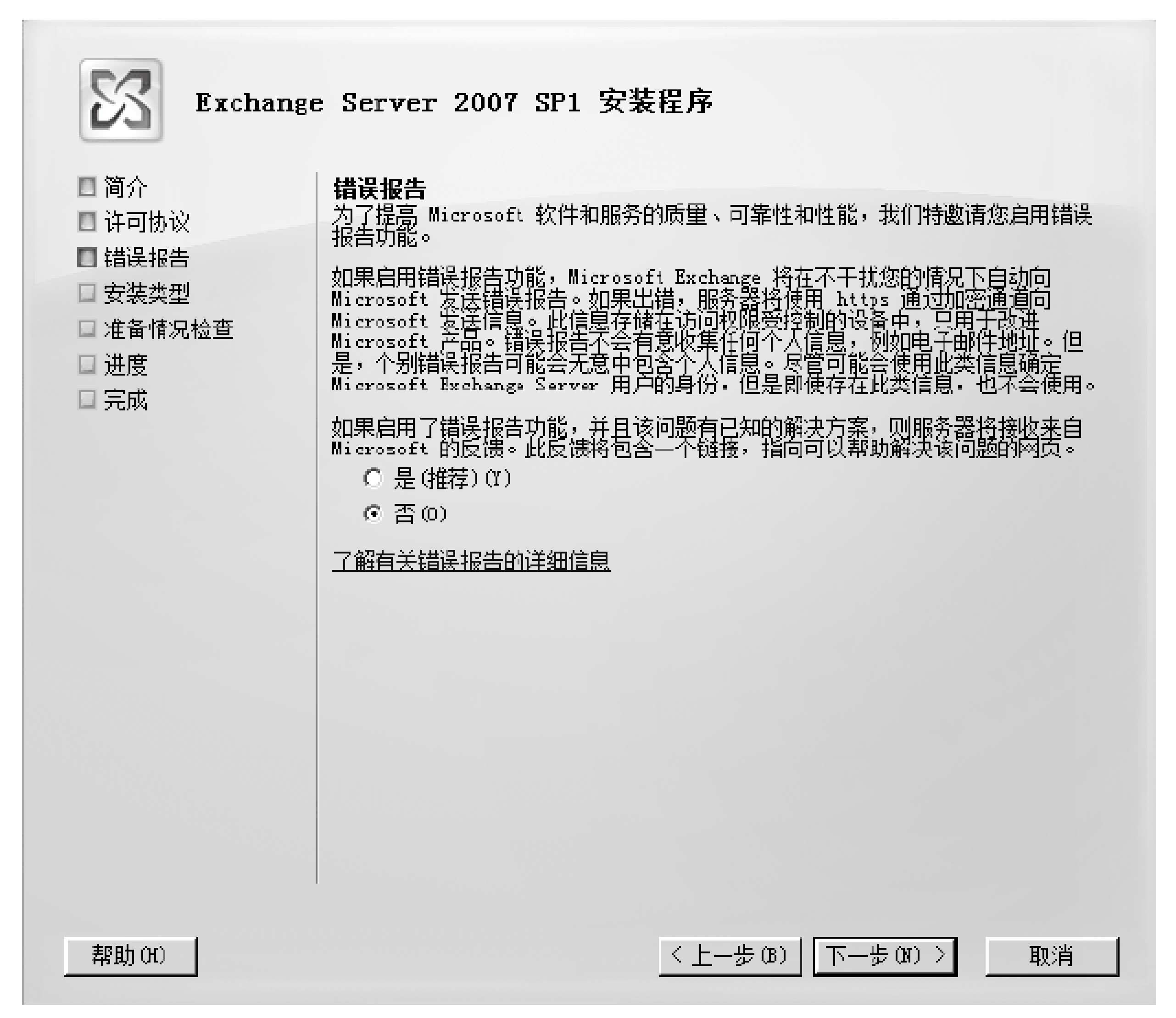


图 10-9　是否启用错误报告功能

(5) 接下来显示“安装类型”界面，如图 10-10 所示，可以选择典型安装，也可以选择自定义安装。如果选择典型安装，系统将自动安装集线器传输服务器角色、客户端访问服务器角色、邮箱服务器角色和 Exchange 管理工具。如果选择自定义安装，则除上述 4 个选项外，又多出统一消息和边缘传输两个角色可供选择。在此选择典型安装，并且安装路径保持默认值不变，然后单击“下一步”按钮。

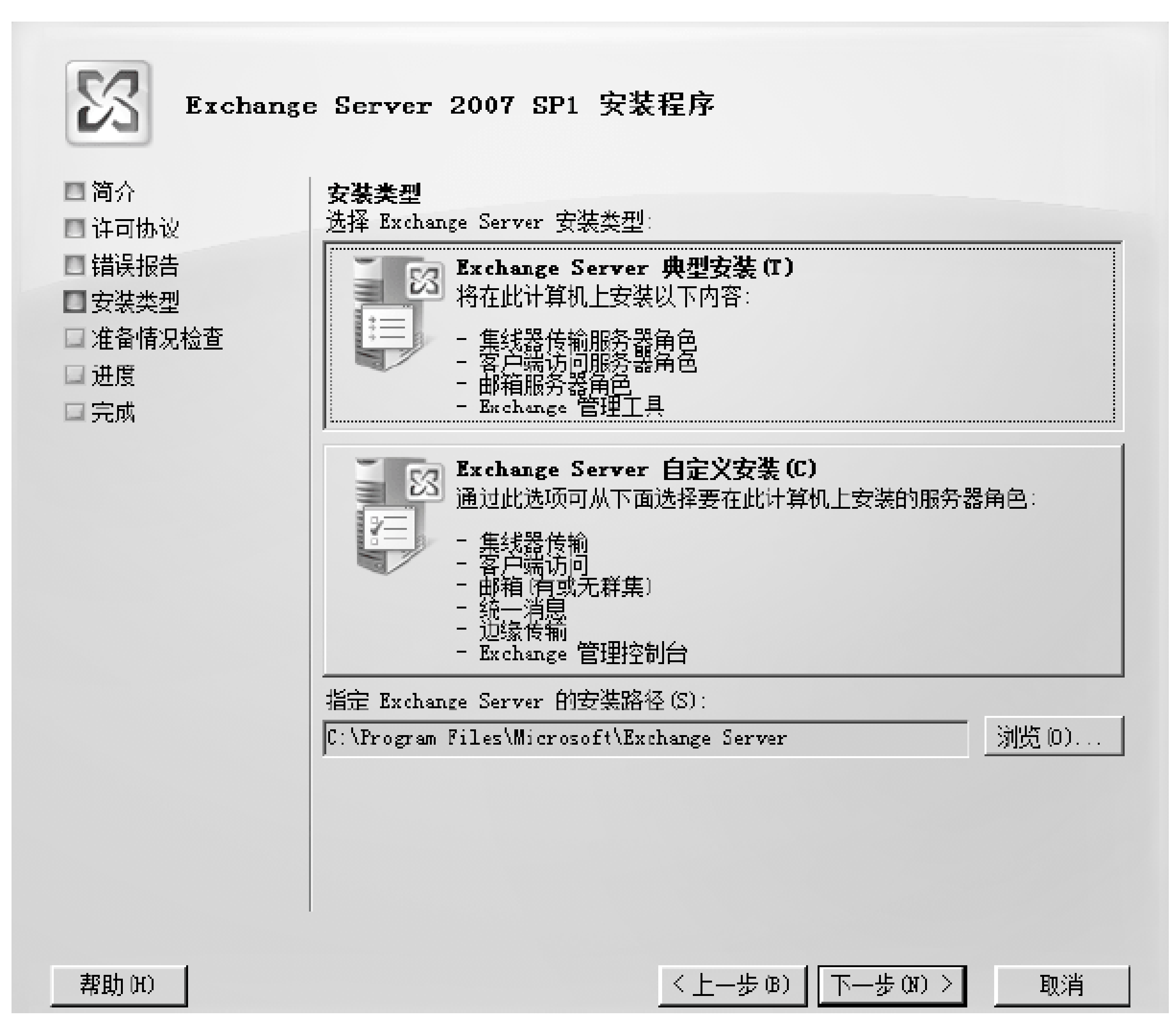


图 10-10　选择安装类型和安装路径

(6) 在下一个界面中，安装程序要求指定 Exchange 组织名称，在此保持默认值 First Organization 不变，然后单击“下一步”按钮，如图 10-11 所示。



图 10-11　指定 Exchange 组织名称

(7) 在下一个界面中询问是否支持早期客户端版本，在此选择“是”，然后单击“下一步”按钮，如图 10-12 所示。

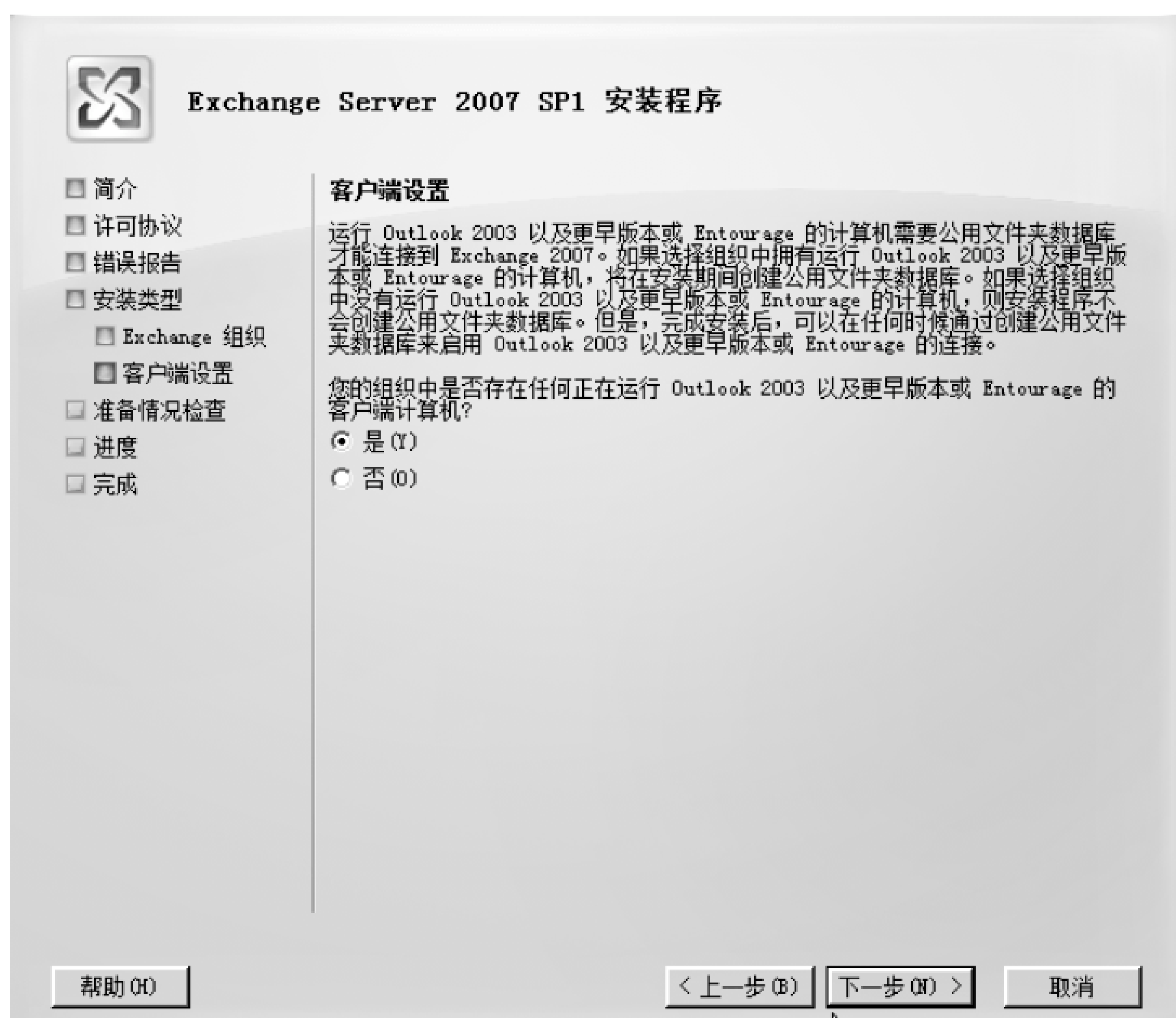


图 10-12　选择支持早期客户端版本

(8) 接下来是准备情况检查，安装程序将对系统进行检查，检查能否成功安装Exchange。在实际安装过程中，这一步经常会检查出一些问题，有的需要安装补丁程序，有的需要启动某个服务，有的需要添加某个组件。

下面是准备情况检查未通过的一个例子。原因是Web服务器的“动态内容压缩”角色服务没有添加，如图10-13所示。

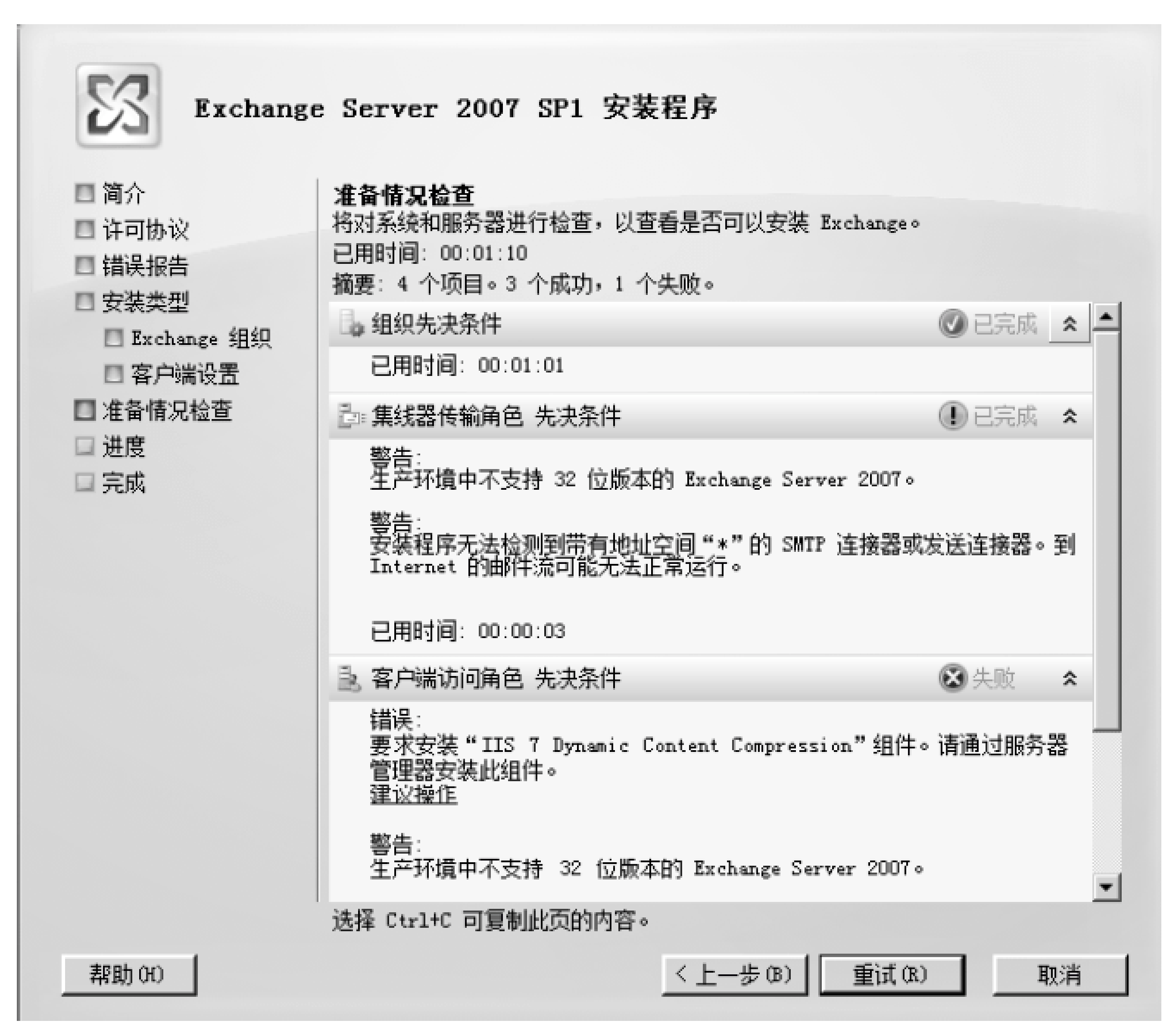


图 10-13　准备情况检查未通过

解决的办法就是打开“服务器管理器”，在左侧窗格中选择“Web 服务器(IIS)”，在右侧的窗格中单击“添加角色服务”，如图10-14所示。



图 10-14　单击“添加角色服务”

在弹出的“添加角色服务”向导中，如图 10-15 所示，选中“动态内容压缩”复选框，单击“下一步”按钮，完成“动态内容压缩”角色服务的添加。

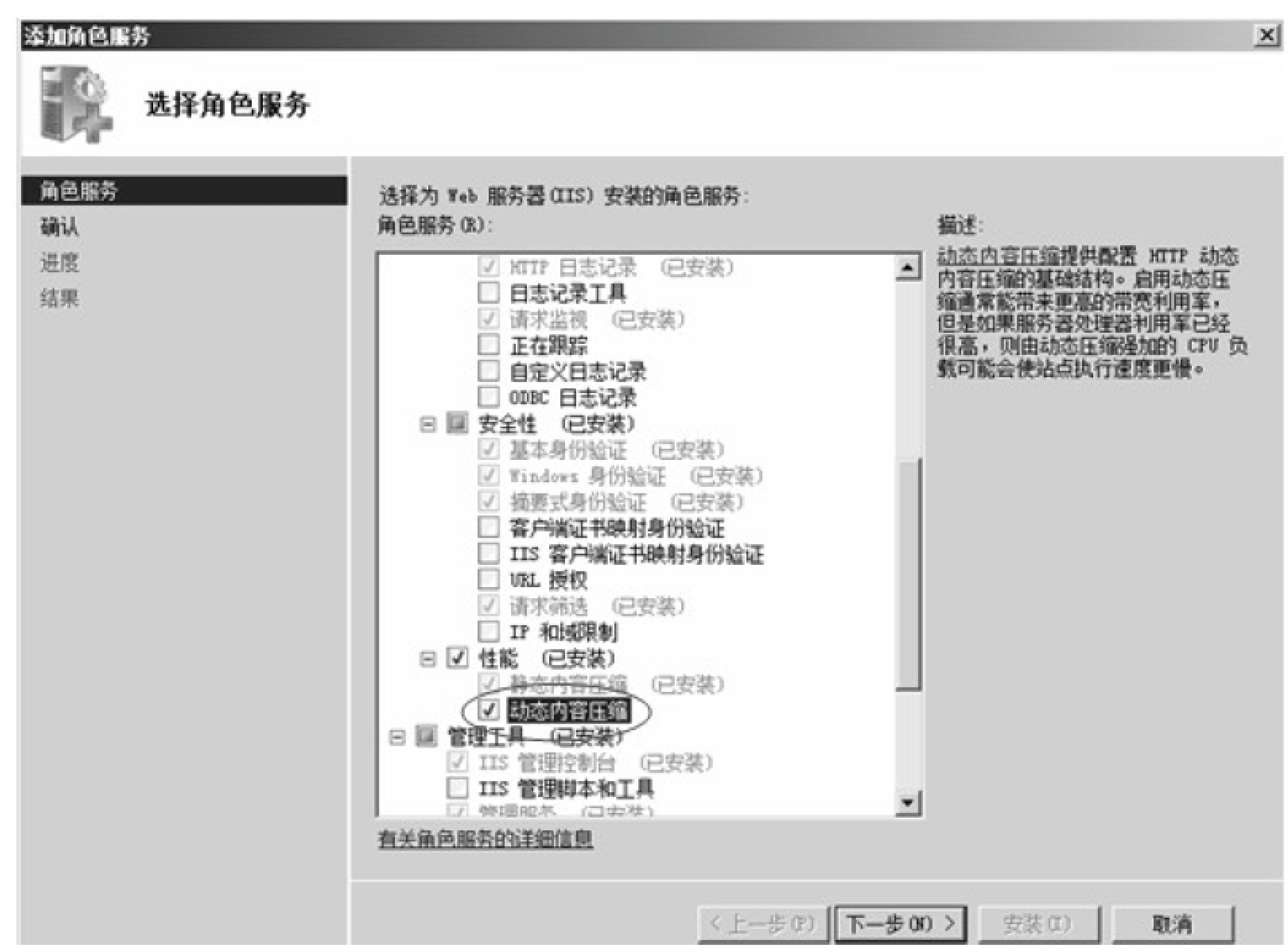


图 10-15　选择“动态内容压缩”

回到如图 10-13 所示的对话框，单击“重试”按钮，完成准备情况检查，如图 10-16 所示，并在此对话框中单击“安装”按钮，继续进行 Exchange 的安装。

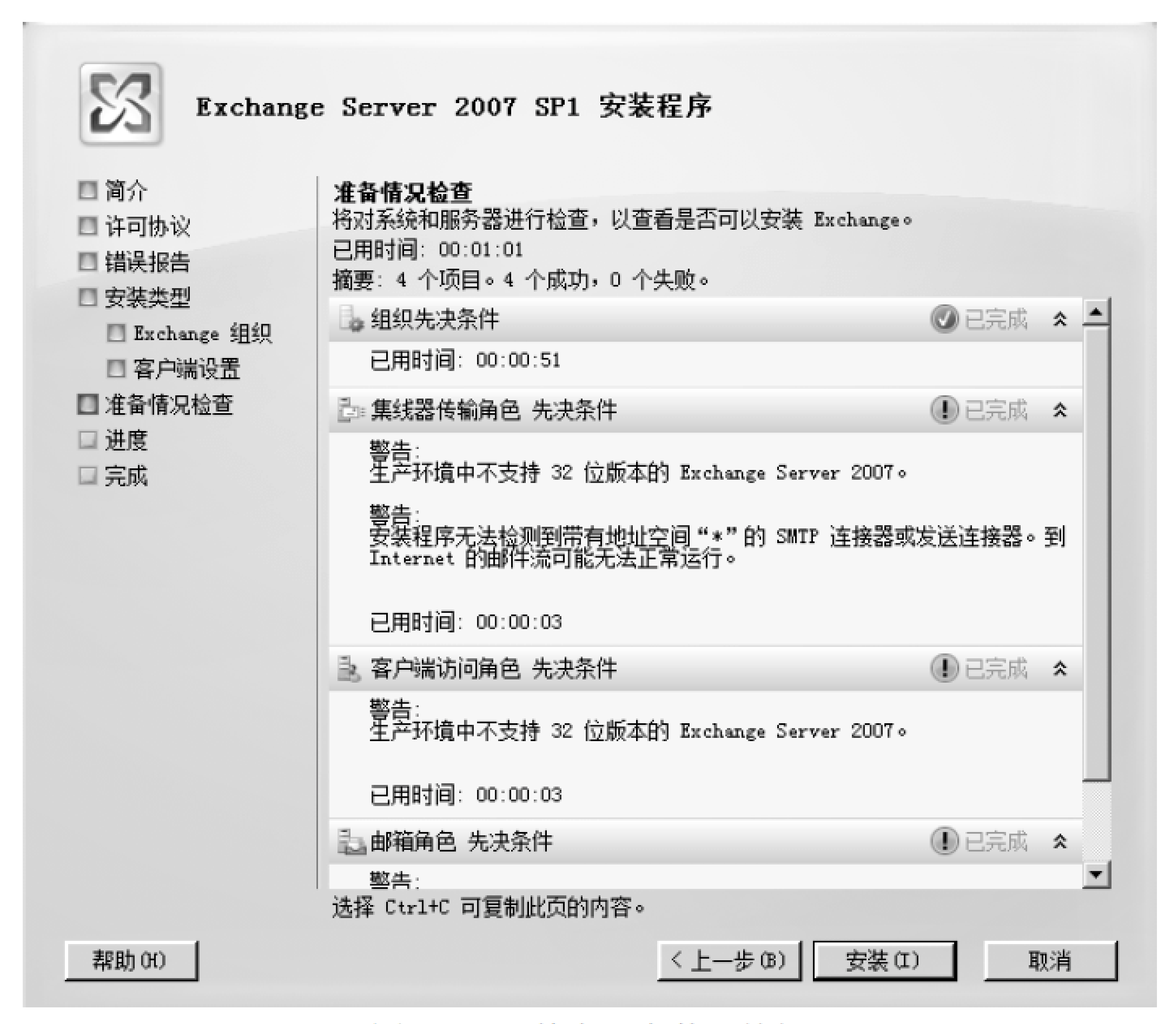


图 10-16　单击“安装”按钮

(9) 经过一段时间的等待，将出现安装完成对话框，如图 10-17 所示。在此对话框中单击“完成”按钮，将返回 Exchange 安装起始对话框，单击“关闭”按钮，重新启动计算机，Exchange Server 2007 SP1 安装结束。

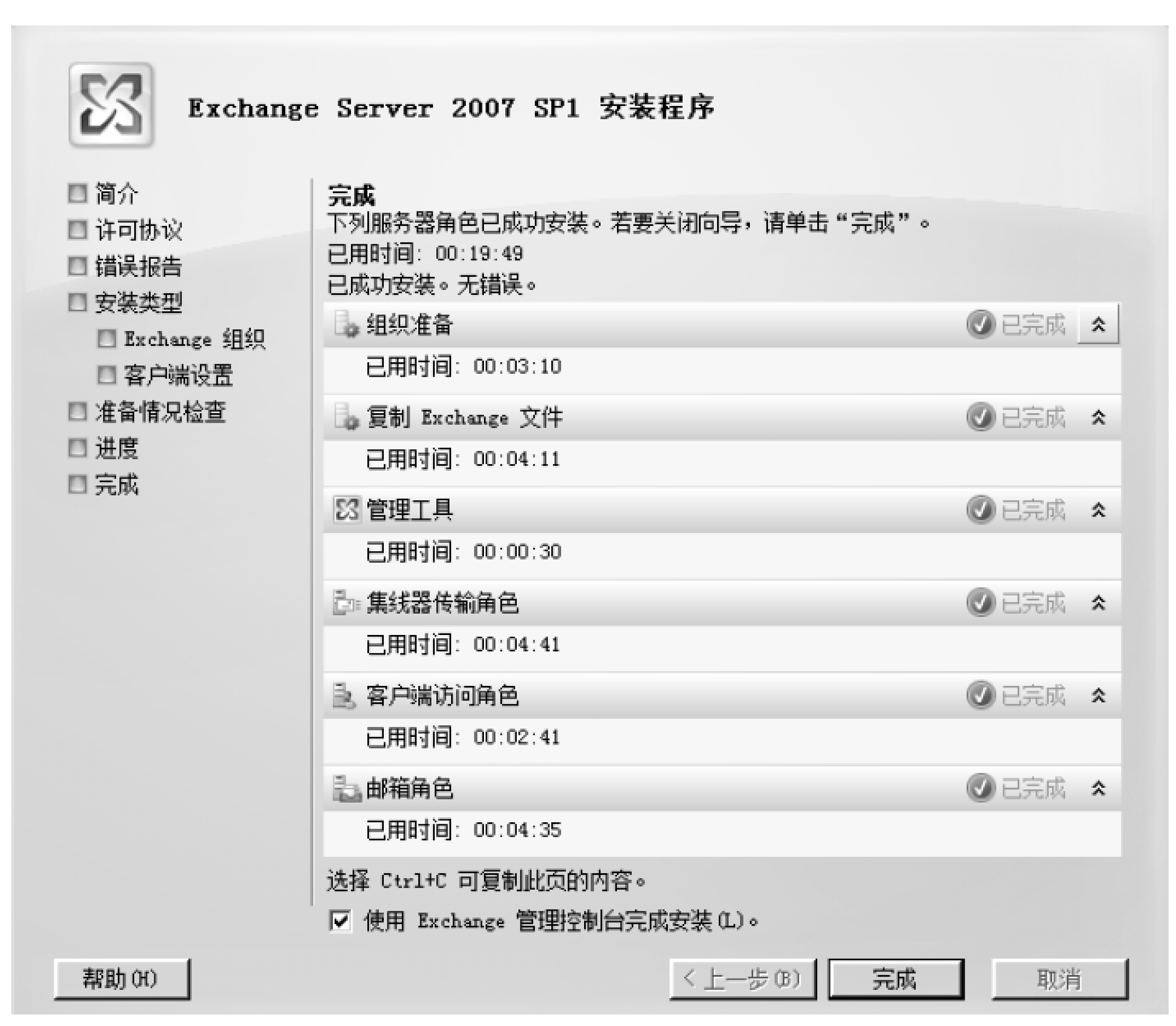


图 10-17　安装完成

安装完成重新启动计算机后，需要确认安装是否正确，有如下项目需要进行检查：

(1) 核对“所有程序”菜单中是否存在“Microsoft Exchange Server 2007”子菜单，其中应该包括“Exchange Server 帮助”、“Exchange 管理控制台”、“Exchange 命令行管理程序”3 项，如图 10-18 所示。其中的“Exchange 管理控制台”和“Exchange 命令行管理程序”是两个非常重要的管理程序，在后续工作中经常使用。

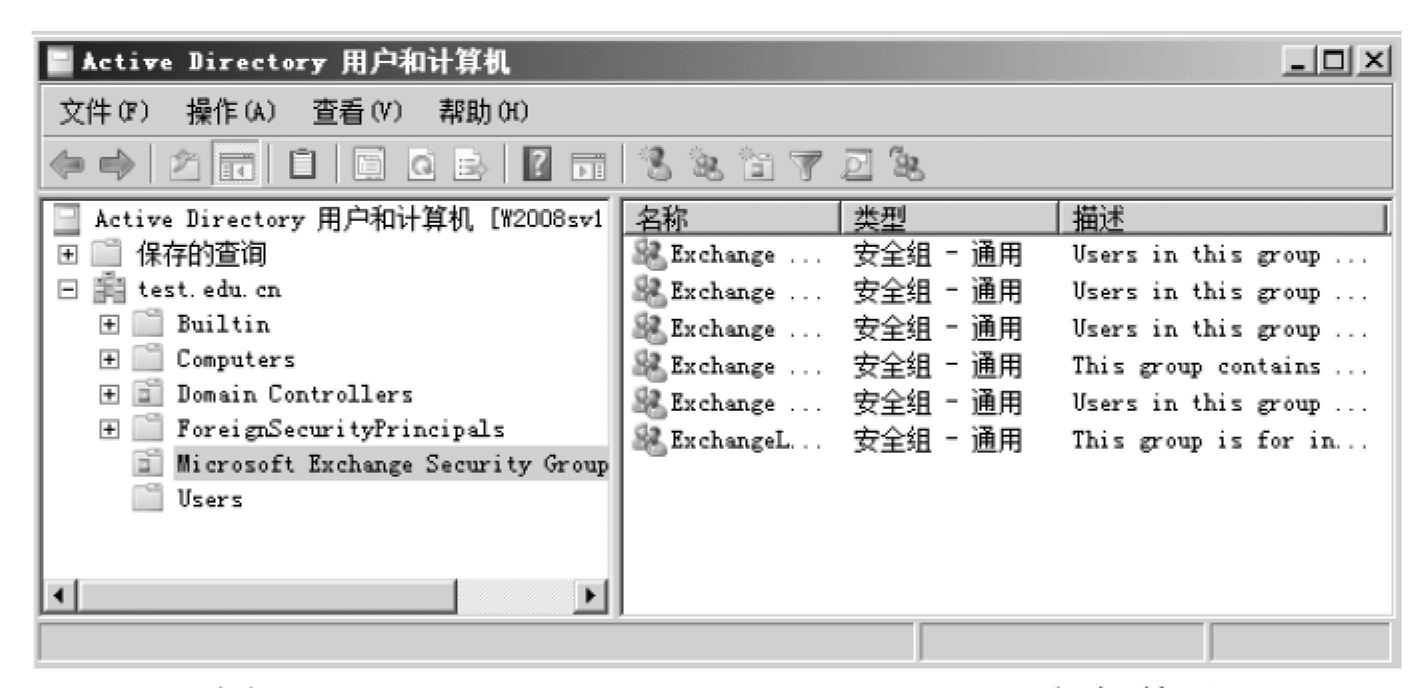


图 10-18　Microsoft Exchange Security Group 组织单元

(2) 核对“Active Directory 用户和计算机”管理窗口中是否出现以“Microsoft Exchange Security Groups”命名的组织单位，其中包含一些 Microsoft Exchange 使用的通用安全组，

如图 10-19 所示。

如果检查通过，系统就可正常使用了。在下一节将使用 Exchange 管理控制台建立邮箱。

Microsoft Exchange Server 2007
Exchange Server 帮助
Exchange 管理控制台
Exchange 命令行管理程序

图 10-19　Microsoft Exchange Server 2007 子菜单

10.3　建立用户邮箱

建立用户邮箱可以使用“Exchange 管理控制台”，也可以使用“Exchange 命令行管理程序”，这里使用“Exchange 管理控制台”来完成这一工作。步骤如下：

(1) 以 Administrator 身份登录域，选择“开始”→“所有程序”→“Microsoft Exchange Server 2007”→“ Exchange 管理控制台”命令，打开“Exchange 管理控制台”窗口，展开“收件人配置”，选择“邮箱”，如图 10-20 所示。

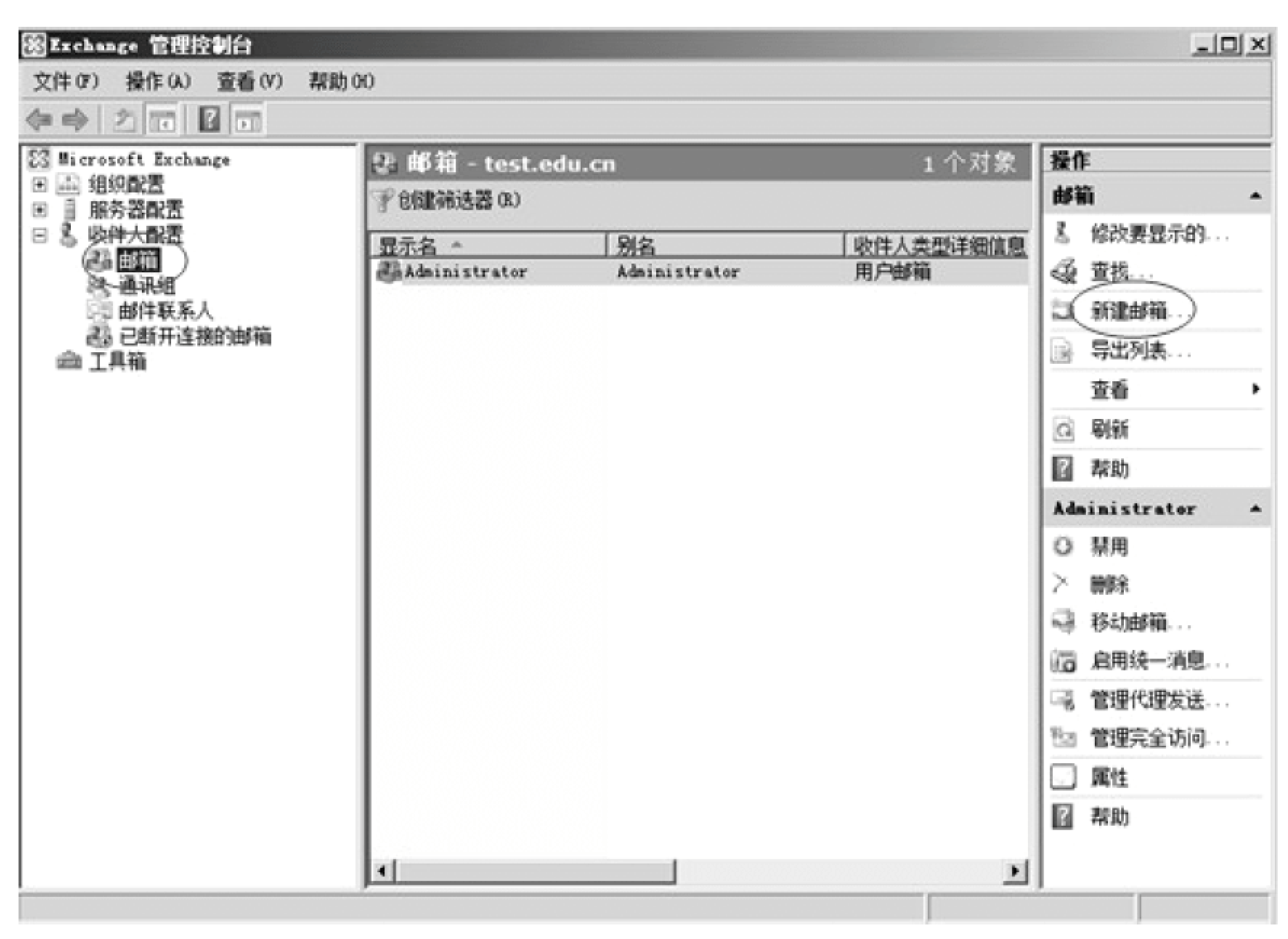


图 10-20　Exchange 管理控制台窗口

(2) 在右侧的窗格中选择“新建邮箱”，系统弹出新建邮箱向导对话框。首先是选择邮箱类型，这里选择“用户邮箱”，然后单击“下一步”按钮，如图 10-21 所示。

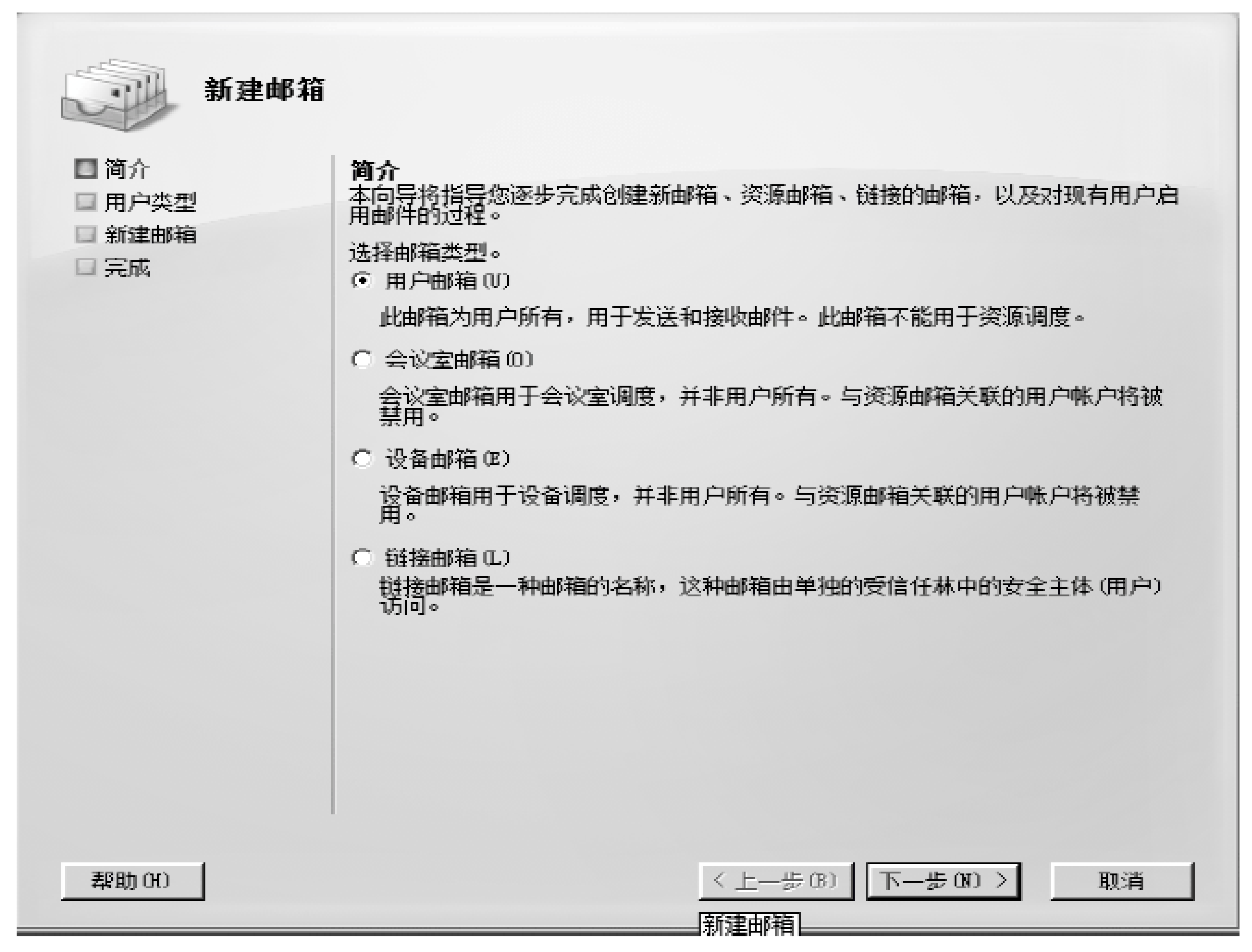


图 10-21　选择邮箱类型

(3) 选择“用户类型”，如图 10-22 所示，可以选择为“新建用户”建立邮箱，也可以选择为“现有用户”建立邮箱。如果选择为“现有用户建立邮箱”，下一步就会要求在域中选择一个现有的用户，否则就自动在域中新建一个用户与新建的邮箱关联，因为在 Exchange Server 2007 中每个邮箱都需要一个域用户与之关联。这里选择“新建用户”，然后单击“下一步”按钮。

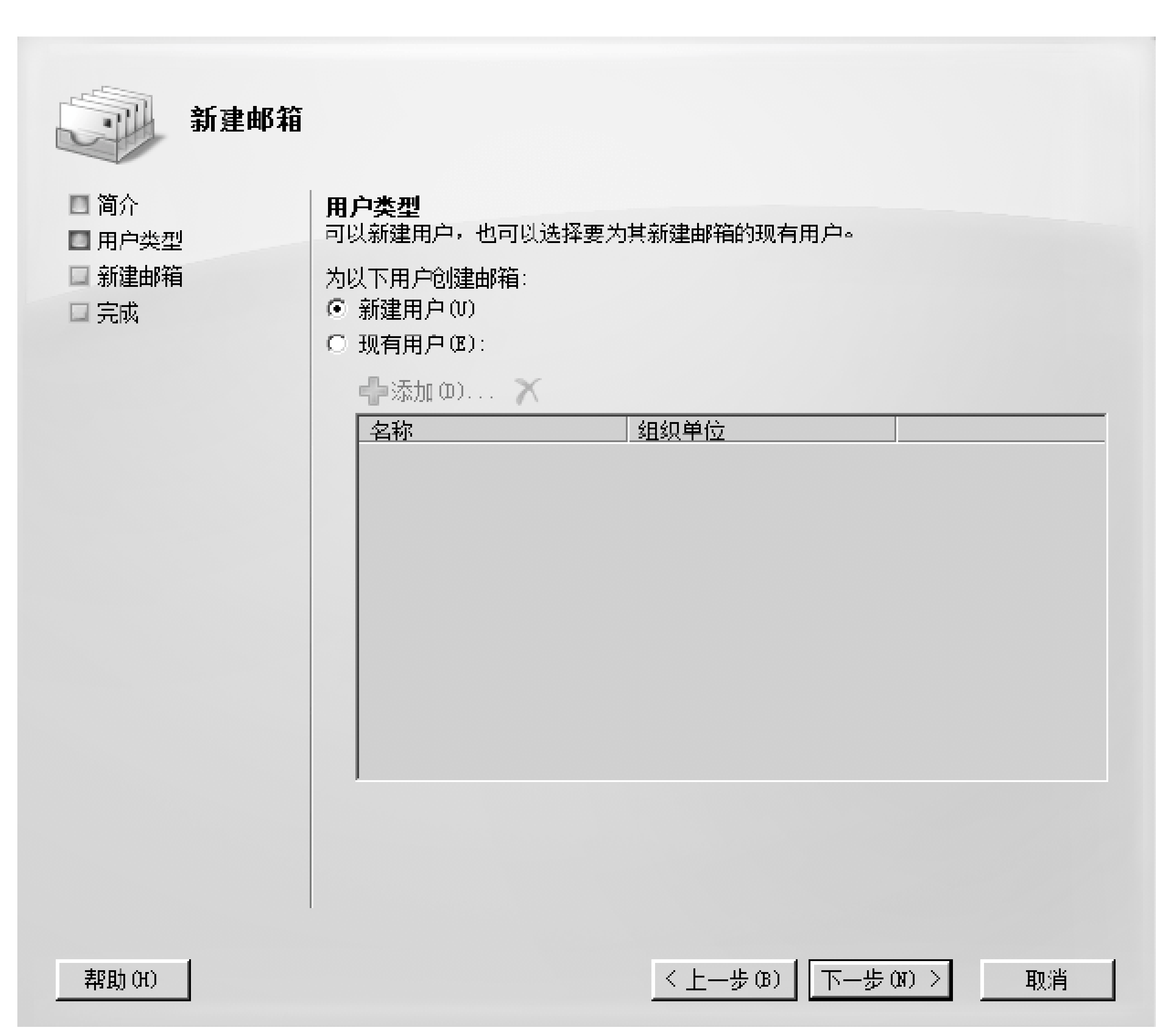


图 10-22　选择用户类型

(4) 如图 10-23 所示，输入用户及所在组织单位的相关信息，单击“下一步”按钮。

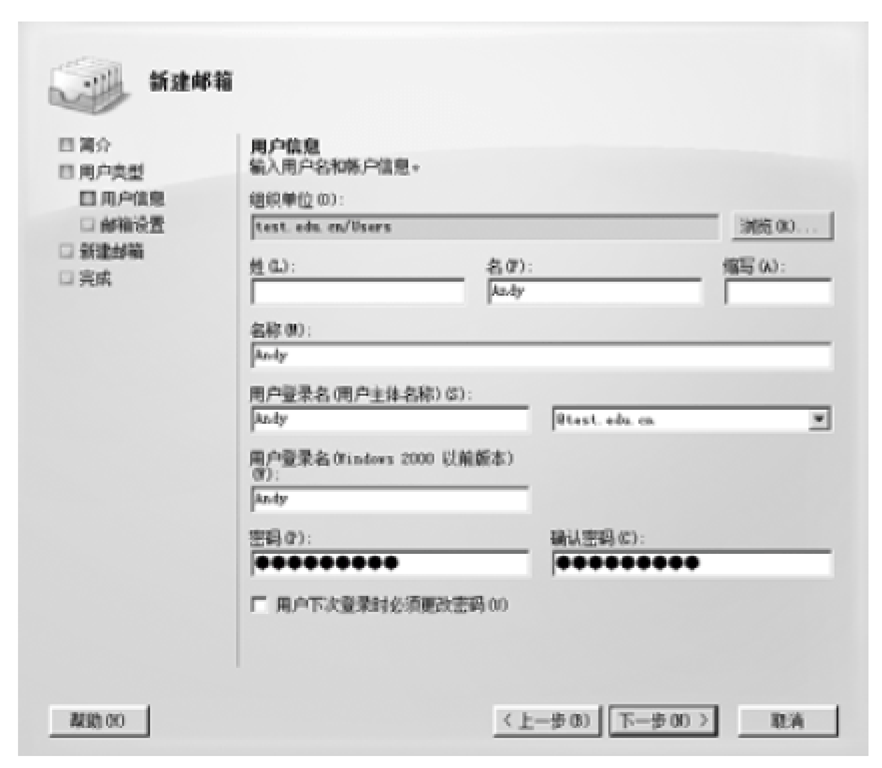


图 10-23　输入用户信息

(5) 在显示的“邮箱设置”对话框中，如图 10-24 所示，其中“别名”字段默认显示“用户登录名(用户主体名称)”，不过可以修改此字段。“邮箱数据库”字段不能为空，必须单击“浏览”按钮选择一个邮箱数据库，此邮箱数据库用于存储新建邮箱的数据，如图 10-25 所示。





图 10-24　邮箱设置　　　　图 10-25　选择邮箱数据库

(6) 选择完成后，如图 10-26 所示，这里可以保留不选中“托管文件夹邮箱策略”和“Exchange ActiveSync 邮箱策略”两个复选框。单击“下一步”按钮。

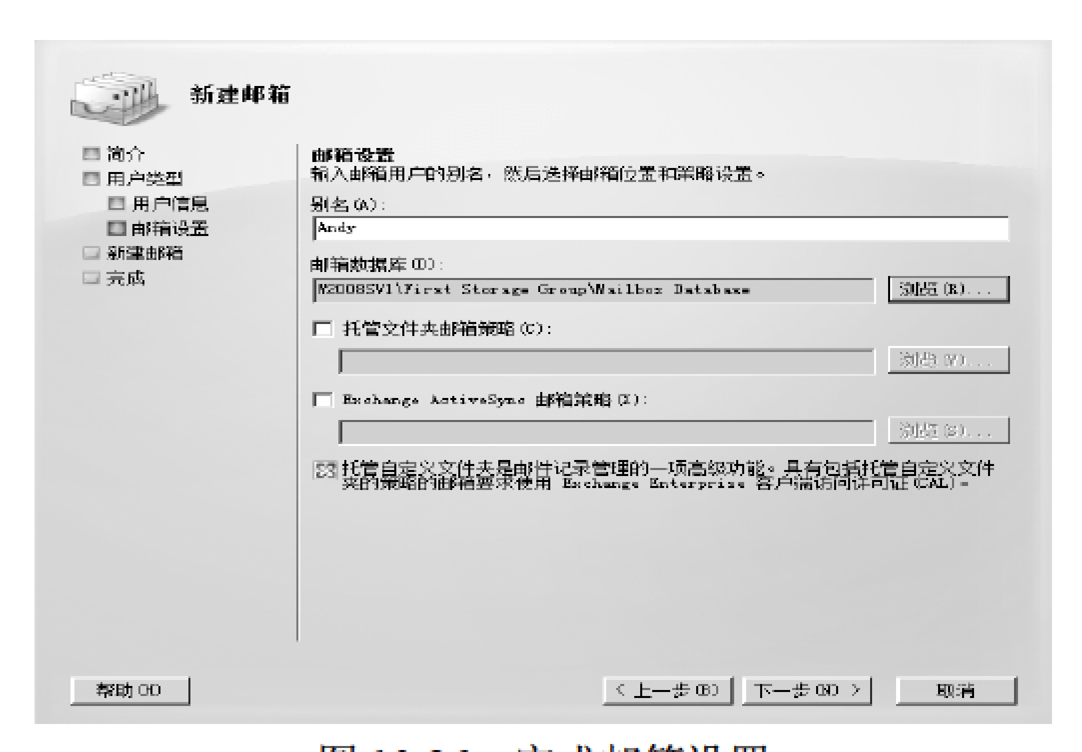


图 10-26　完成邮箱设置

(7) 如图 10-27 所示，阅读摘要后，如果要修改配置内容，可以单击“上一步”按钮。如果不修改，就单击“新建”按钮。



图 10-27　完成邮箱设置

(8) 最后出现“完成”界面，在此可以查看邮箱是否建立成功，同时也显示建立邮箱的 Exchange 命令行管理程序命令，如图 10-28 所示。



图 10-28　“完成”对话框

(9) 单击“完成”按钮后回到 Exchange 管理控制台，在此可以看到新建的用户邮箱，如图 10-29 所示。

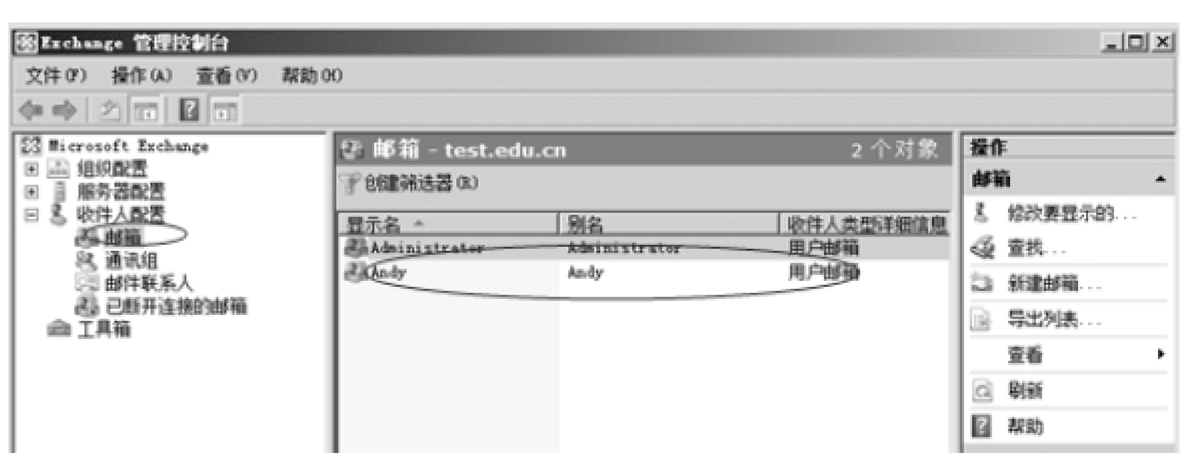


图 10-29　新建的用户邮箱

与新建邮箱关联的域用户可以在“Active Directory 用户和计算机”窗口中看到，如图

10-30 所示。



图 10-30　与新建邮箱关联的域用户

用同样的方法再建立一个邮箱，地址是 Peter@test.edu.cn。

10.4　客户端的使用

10.4.1　使用 OWA 收发邮件

OWA 是 Outlook Web Access 的缩写。在安装 Exchange 服务器时，已经在服务器上创建了一个 Web 站点。选择“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”命令，依次展开“网站”→“Default Web Site”，如图 10-31 所示，可以看到其中有一个 owa 虚拟目录，客户端可以通过浏览器连接这一虚拟目录，只要通过身份验证，就能访问其个人邮箱，并进行邮件收发。



图 10-31　IIS 管理器窗口显示 owa 虚拟目录

下面操作的一台客户机安装的是 Windows XP 操作系统。打开“本地连接”的“TCP/IP 属性”对话框，使用固定 IP 地址设置，如图 10-32 所示。客户机的 IP 地址设为 192.168.1.103，首选 DNS 服务器地址设为 192.168.1.100(本章把域控制器、Exchange 服务器、DNS 服务器安装在同一台计算机上，其 IP 地址是 192.168.1.100)，设置完成后，必须保证在客户端能 ping 通 192.168.1.100，如图 10-33 所示。

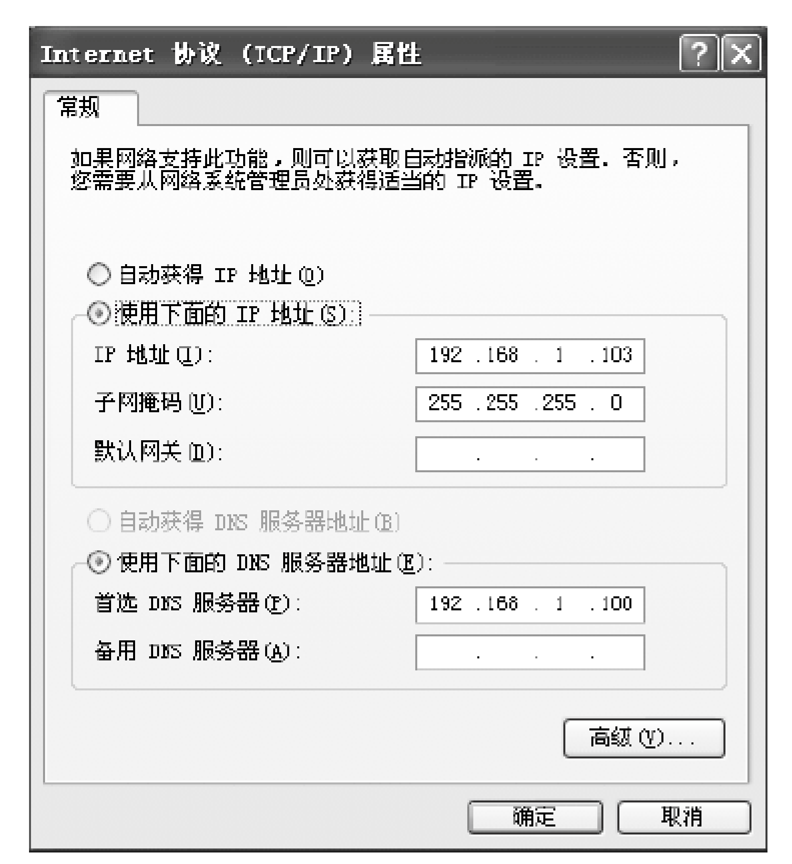


图 10-32　Windows XP 客户端 IP 地址设置

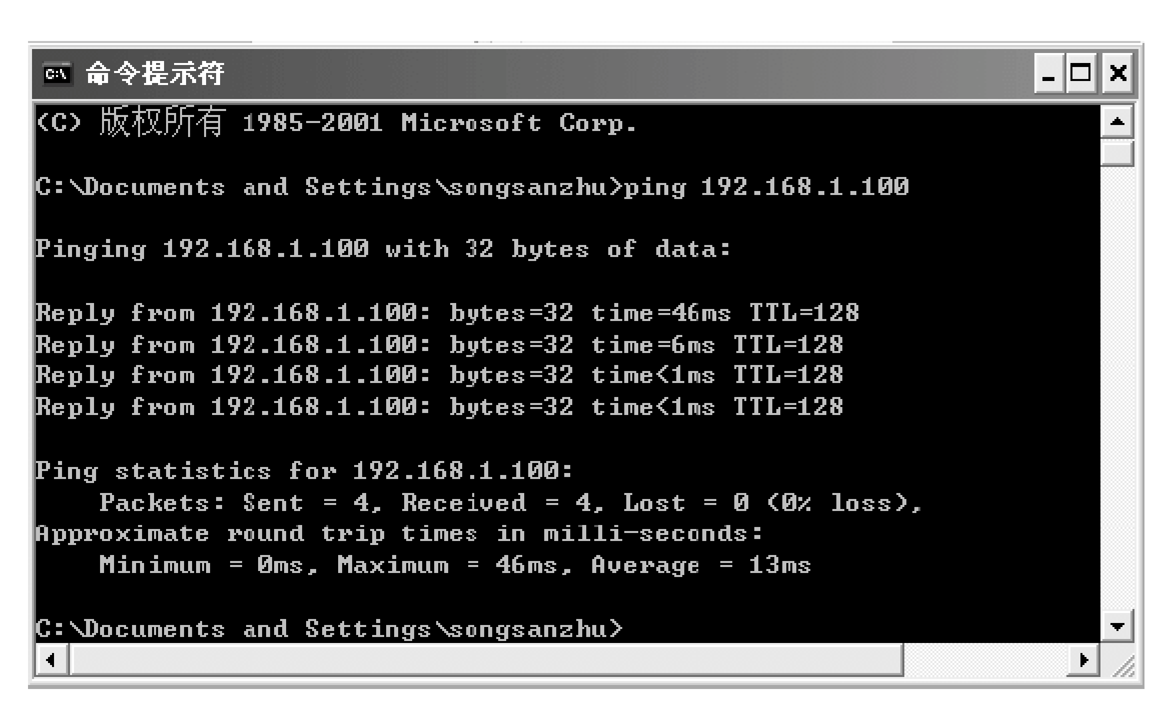


图 10-33　客户端执行 ping 命令的结果

在 DNS 服务器上 w2008sv1.test.edu.cn 应该能解析成 192.168.1.100，如图 10-34 所示。



图 10-34　w2008sv1.test.edu.cn 在 DNS 中的解析

接下来在客户机上打开 IE 浏览器，在地址栏中输入 https://w2008sv1.test.edu.cn/owa，此时会看到“此网站的安全证书有问题”的提示，如图 10-35 所示。这是由于 Exchange 服务器与客户机之间采用加密通信，需要在服务器上安装“安全证书”，在 Exchange 服务器安装过程中，安装了一个自签的安全证书，但并非公共信任的证书，所以才出现这个提示。可以忽略它，单击“继续浏览此网站”。

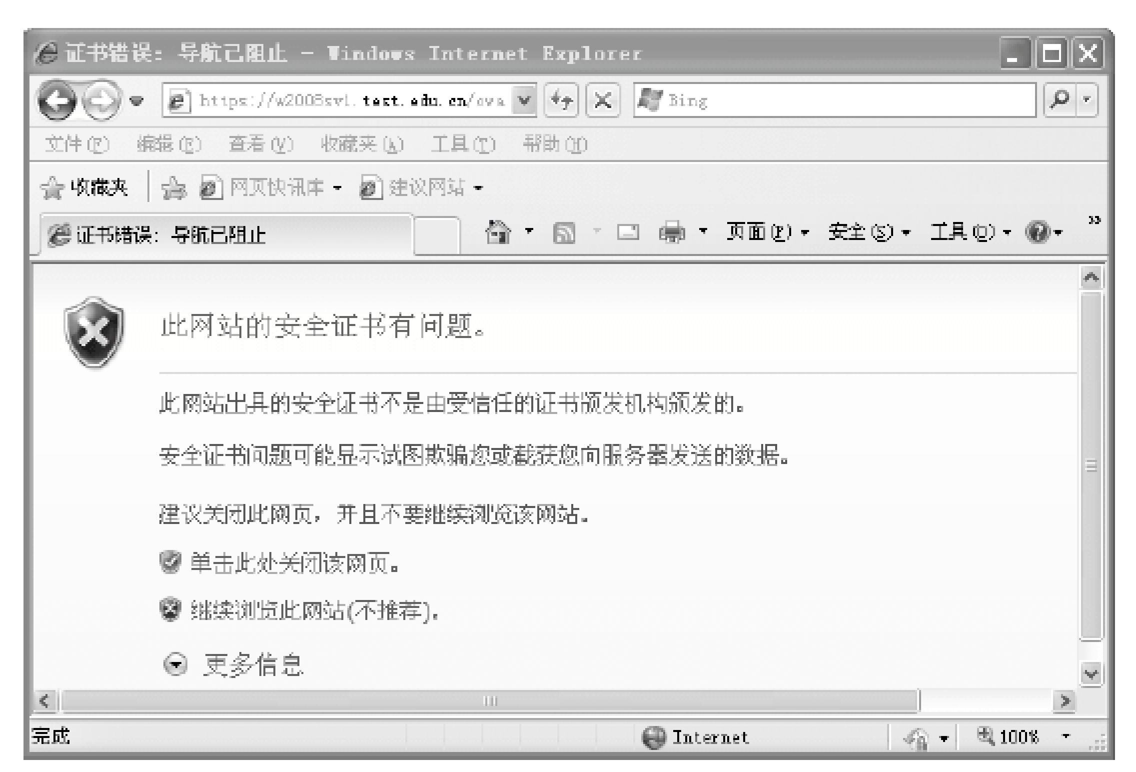


图 10-35　连接 owa 站点

接下来显示 Office Outlook Web Access 登录页面，如图 10-36 所示。输入用户名和密码，然后单击“登录”按钮。

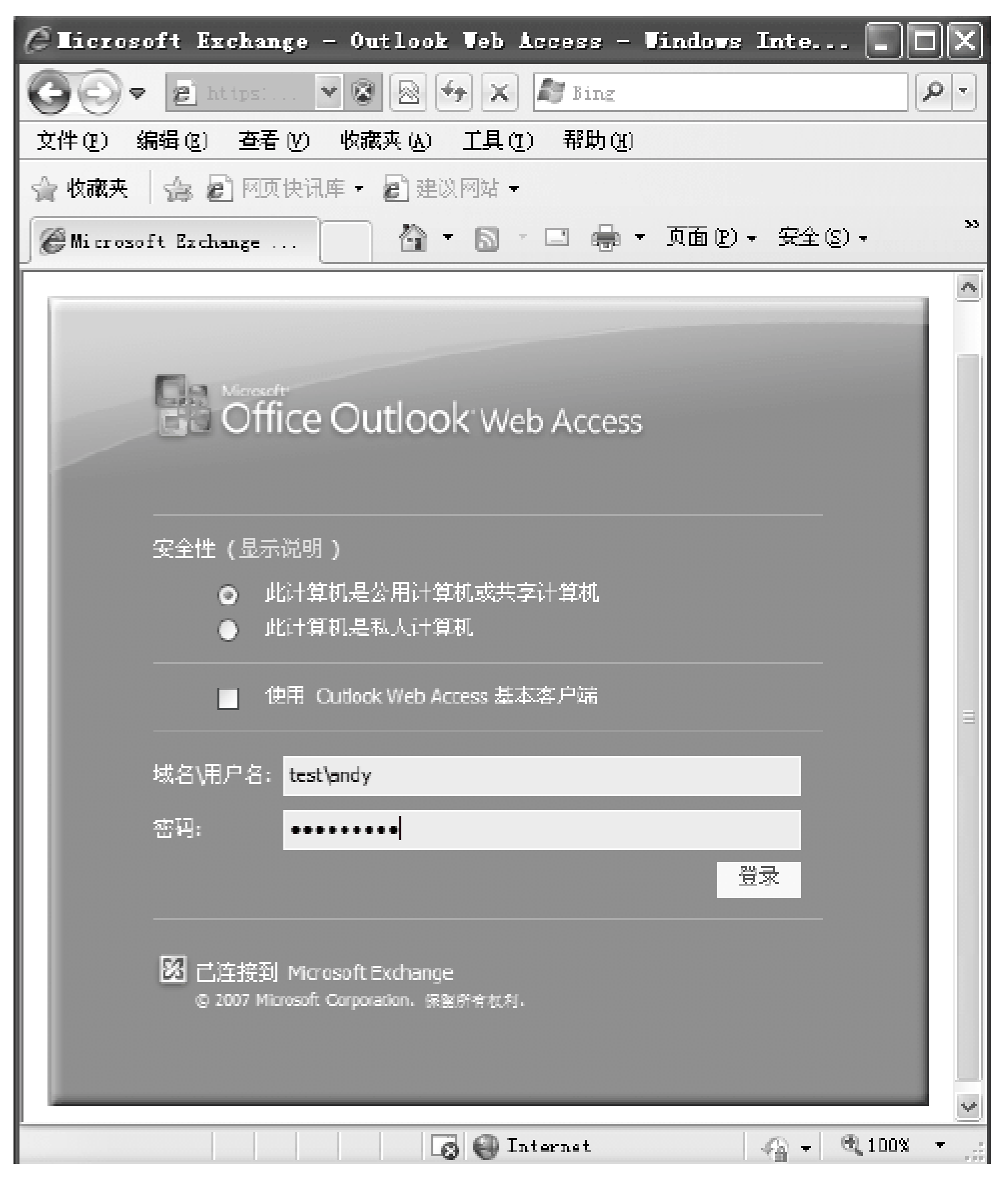


图 10-36　Office Outlook Web Access 登录页面

在语言和时区选择页面，选择后单击“确定”按钮，如图 10-37 所示。



图 10-37　语言和时区选择页面

下面就进入了 Andy 的个人邮箱，如图 10-38 所示。

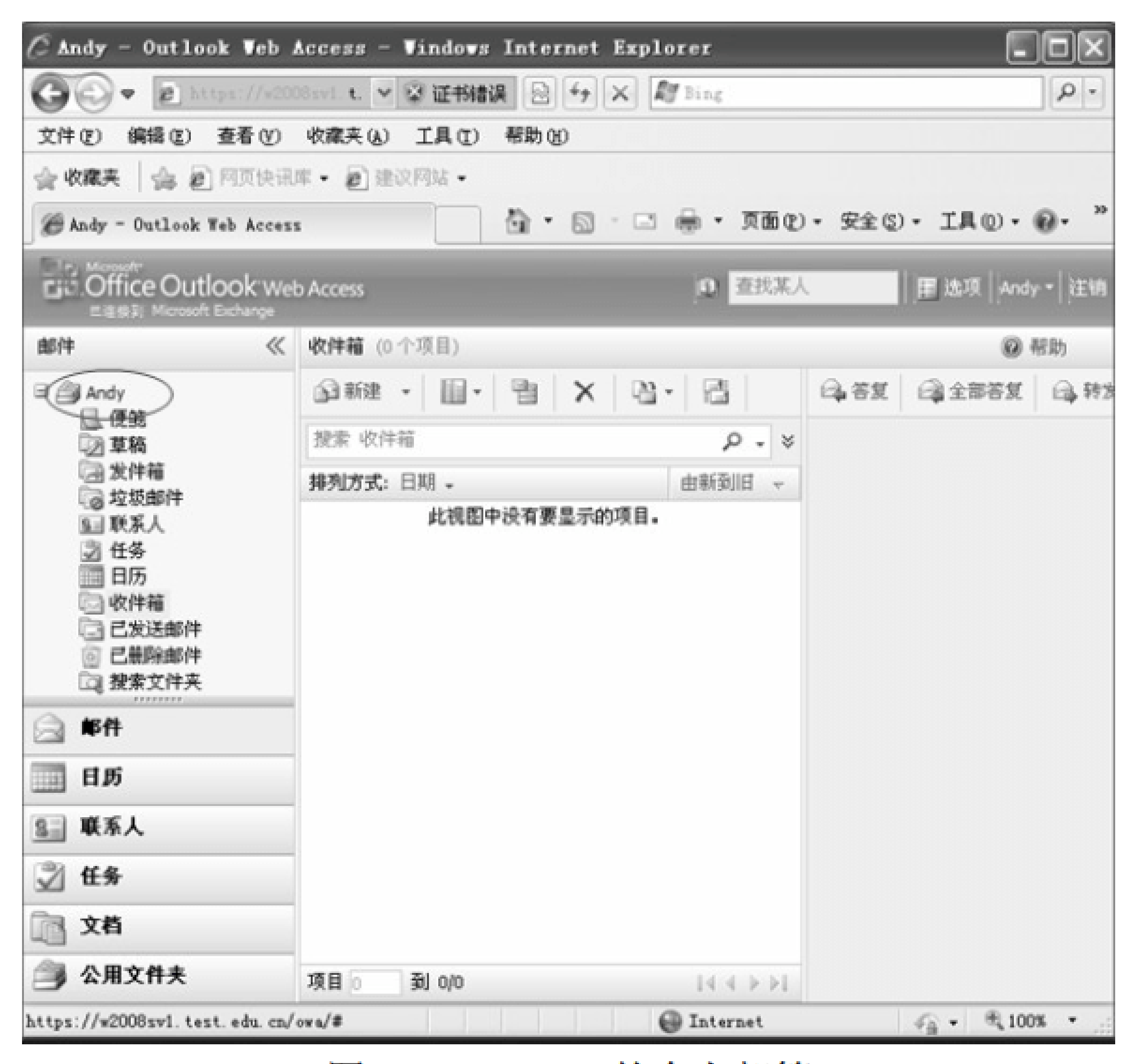


图 10-38　Andy 的个人邮箱

进入个人邮箱后，可以完成很多工作，但本节的重点是基本的邮件收发功能，因此其他功能暂且不提。要发送一封邮件，可以单击“新建”按钮，接下来会出现邮件书写页面，如图 10-39 所示。

在这里可以输入需要的主题，书写邮件的内容，可以在收件人栏中直接手工填入收件人的邮箱地址，还可以单击“收件人”，在弹出的“通讯簿”对话框中选择收件人，如图 10-40 所示。在此对话框中双击 Peter，选择 Peter 作为收件人，然后单击“确定”按钮返回

邮件书写页面。

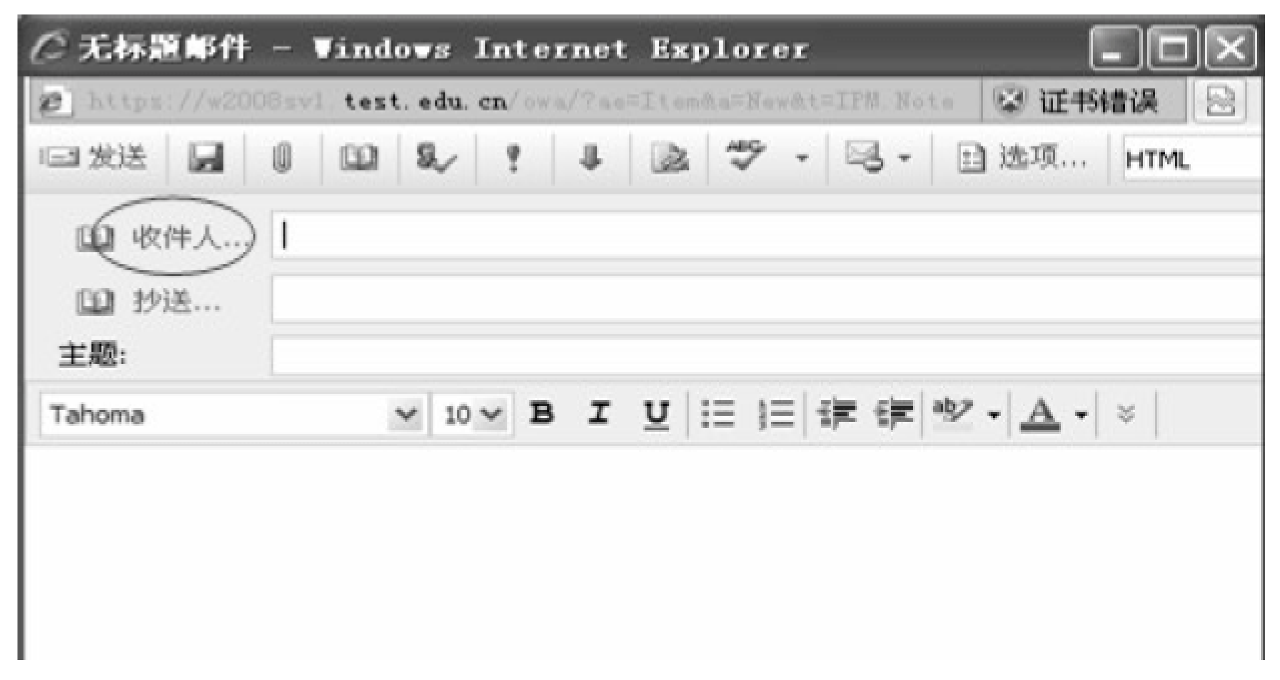


图 10-39　邮件书写页面



图 10-40　通讯簿对话框

返回邮件书写页面后，输入相应内容，如图 10-41 所示。最后单击“发送”按钮来完成邮件的发送。



图 10-41　邮件发送

接下来单击邮箱页面右上角处的“注销”按钮。注销之后再以 Peter 登录，进入 Peter 的个人邮箱，如图 10-42 所示。在此能够看到 Andy 发过来的邮件，双击该邮件就能看到邮件的内容，如图 10-43 所示。



图 10-42　双击 Andy 发来的邮件



图 10-43　阅读邮件的页面

10.4.2　Outlook 的使用

使用 owa 可以在客户端进行邮件收发，使用 Outlook 2007 也能在客户端进行邮件收发。使用 owa 时，只要客户端有 IE 浏览器就不需要再安装额外的软件了。但是，使用 Outlook 2007 则必须在客户端安装 Outlook 2007 软件，不过 Outlook 2007 的功能更丰富，界面更漂亮。下面要操作的是网络中的另外一台计算机，安装的操作系统是 Windows Server 2003。步骤如下：

(1) 首先进行 IP 地址的设置，如图 10-44 所示。然后要保证能 ping 通 192.168.1.100。

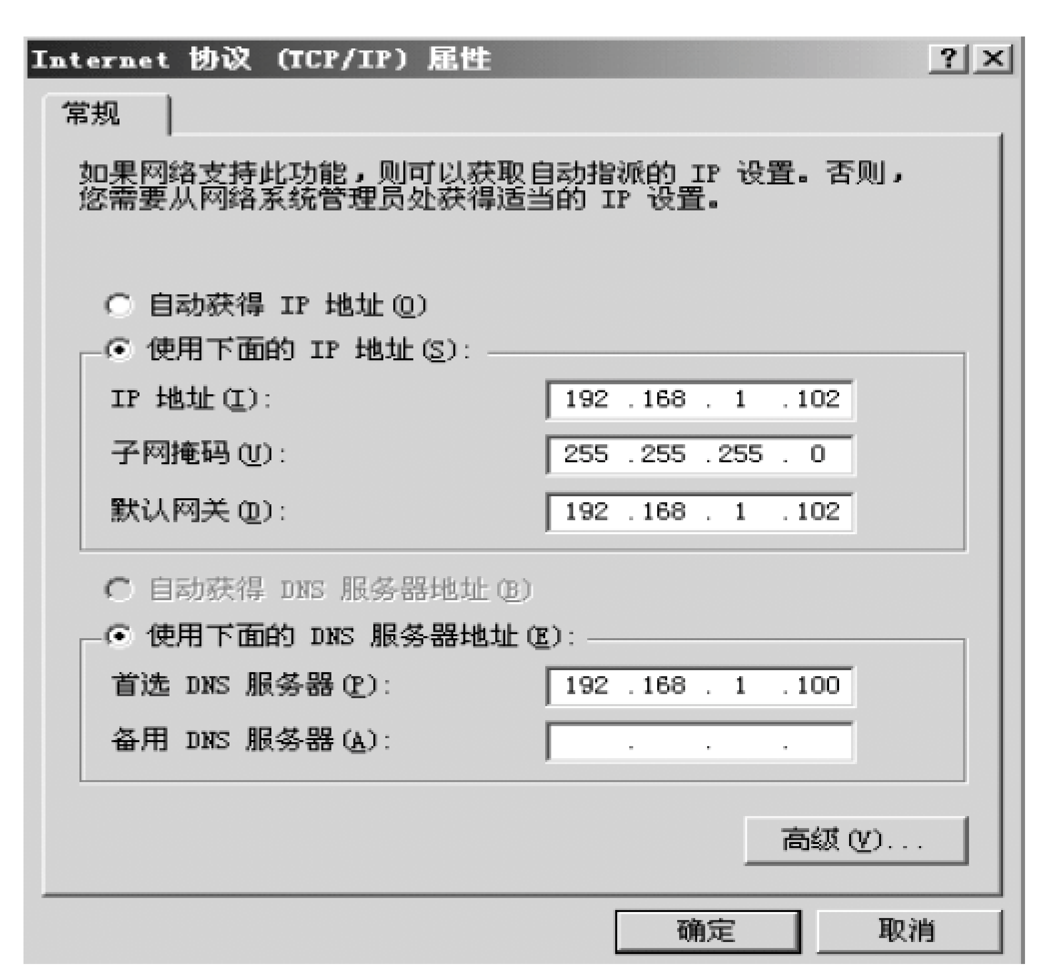


图 10-44　IP 地址设置

(2) 在 DNS 服务器中要添加一条 A 类型的记录，确保把 autodiscover.test.edu.cn 解析为 192.168.1.100，如图 10-45 所示。这是 Outlook 2007 客户端进行“自动配置”所需要的一个重要步骤。



图 10-45　解析 autodiscover.test.edu.cn

(3) 这里不介绍 Outlook 2007 的安装，假定此计算机并未加入域，且 Outlook 2007 的安装已经完成。下面介绍 Outlook 启动时，进行登录所需要的“电子邮件帐户”的配置过程。在控制面板中选择“邮件”命令，如图 10-46 所示。



图 10-46　选择“邮件”命令

(4) 弹出“邮件设置”对话框，在此对话框中单击“电子邮件帐户”按钮，如图 10-47 所示。



图 10-47　单击“电子邮件帐户”按钮

(5) 在弹出的帐户设置对话框中，打开“电子邮件”选项卡，单击“新建”按钮，如图 10-48 所示。

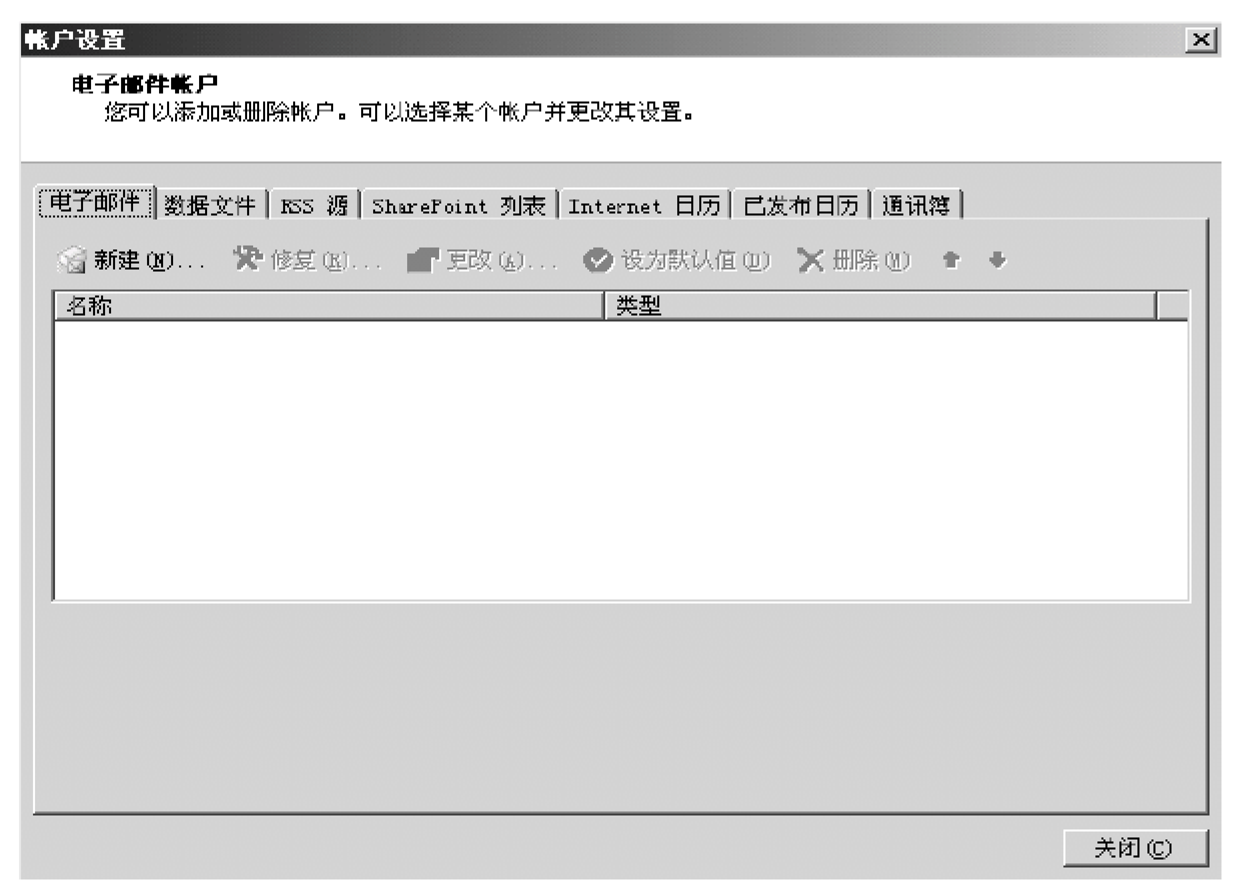


图 10-48　打开“电子邮件”选项卡

(6) 在选择“电子邮件服务”界面中，选择第一项，如图 10-49 所示，然后单击“下一步”按钮。



图 10-49　选择电子邮件服务

(7) 在“自动帐户设置”界面中，输入姓名、邮件地址、密码，但不要选中“手动配置服务器设置或其他服务器类型”，如图 10-50 所示，然后单击“下一步”按钮。

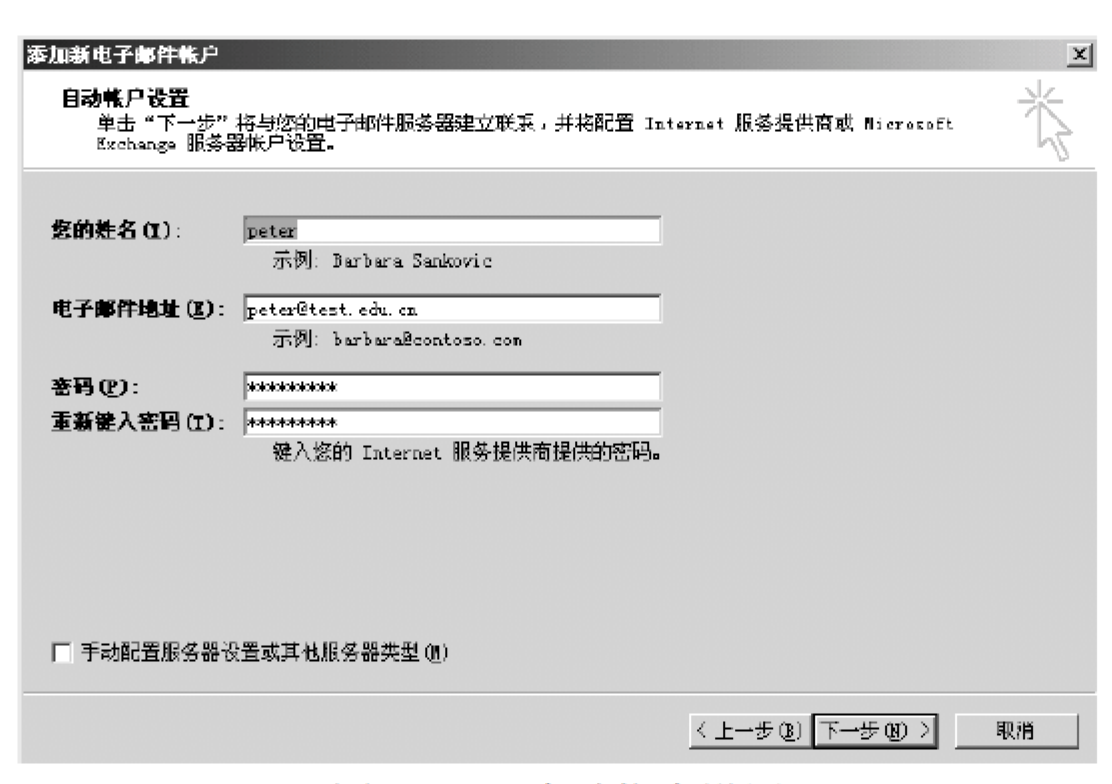


图 10-50　自动帐户设置

(8) 紧接着显示“正在配置”界面，如果 autodiscover.test.edu.cn 不能被正确解析，自动配置过程就不可能成功。本章开始进行了正确的 DNS 配置，因此这里的自动配置也顺利完成，如图 10-51 所示。然后单击“完成”按钮。



图 10-51　正在配置

(9) 下边显示“邮件送达位置”对话框，在其中单击“确定”按钮，如图 10-52 所示。



图 10-52　邮件送达位置

(10) 此时返回“帐户设置”对话框，如图 10-53 所示，然后单击“关闭”按钮，完成电子邮件帐户的设置。



图 10-53　“帐户设置”对话框

对于“安全警告”的说明：如图 10-54 所示的安全警告，是由于安全证书问题引起的，它会在 Outlook 2007 的配置和使用过程中偶尔出现。在本书的实验环境中，对于这种现象可以忽略，直接选择继续，这样不会影响邮件的收发。

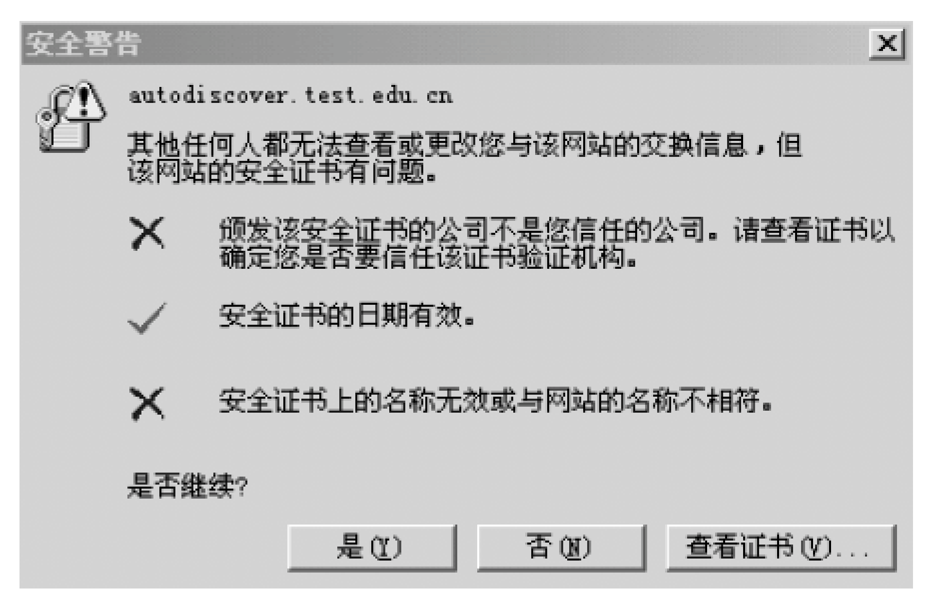


图 10-54　安全警告

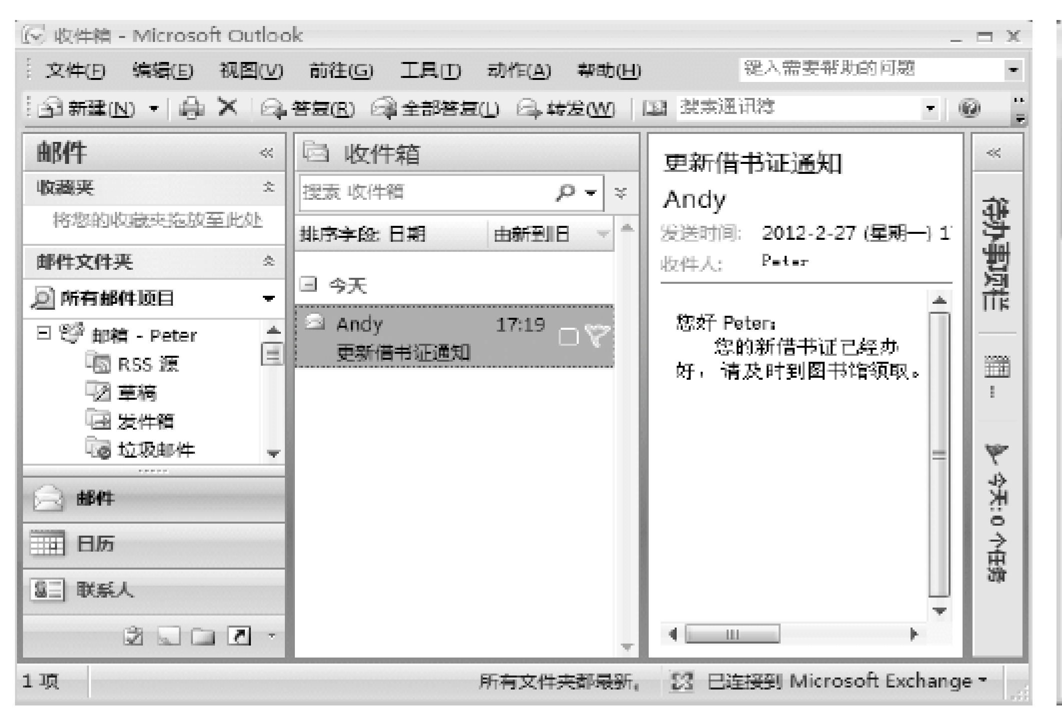
(11) 下边启动 Outlook 2007，选择“开始”→“所有程序”→“Microsoft Office”→“Microsoft Office Outlook 2007”命令，立刻就会弹出一个登录对话框，如图 10-55 所示，在此对话框中输入刚刚配置好的用户名和对应的密码，然后单击“确定”按钮。



图 10-55　登录对话框

(12) 接下来进入 Peter 的个人邮箱，如图 10-56 所示，在此也能看到 Andy 发来的邮件，因为不管是 owa 还是 Outlook 打开的都是 Peter 的个人邮箱，因此看到的邮件是相同的。

如果要发一份送邮件，就单击左上角的“新建”按钮，系统会弹出邮件书写窗口，如图 10-57 所示。



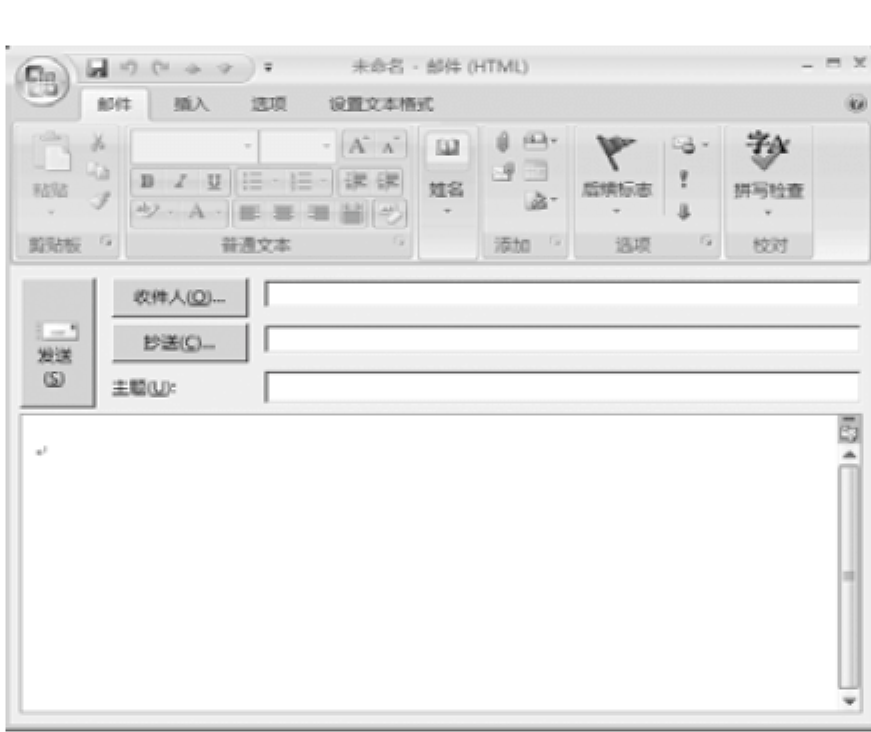



图 10-56　Outlook 的主窗口　　图 10-57　Outlook 的邮件书写窗口

(13) 在邮件书写窗口中，单击“收件人”按钮，将弹出“全球通讯簿”对话框，在其中双击 Andy，选 Andy 作为收件人，再单击“确定”按钮，如图 10-58 所示。

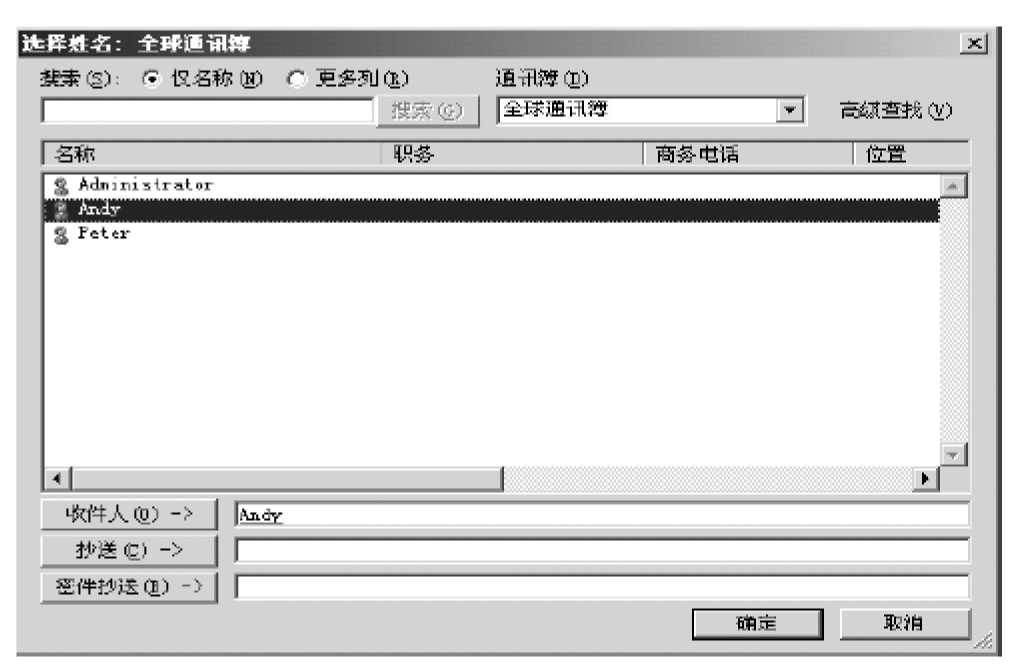


图 10-58　通讯簿对话框

(14) 下面在邮件书写窗口中填写邮件内容，然后单击“发送”按钮，将邮件发送到 Andy 的邮箱，如图 10-59 所示。

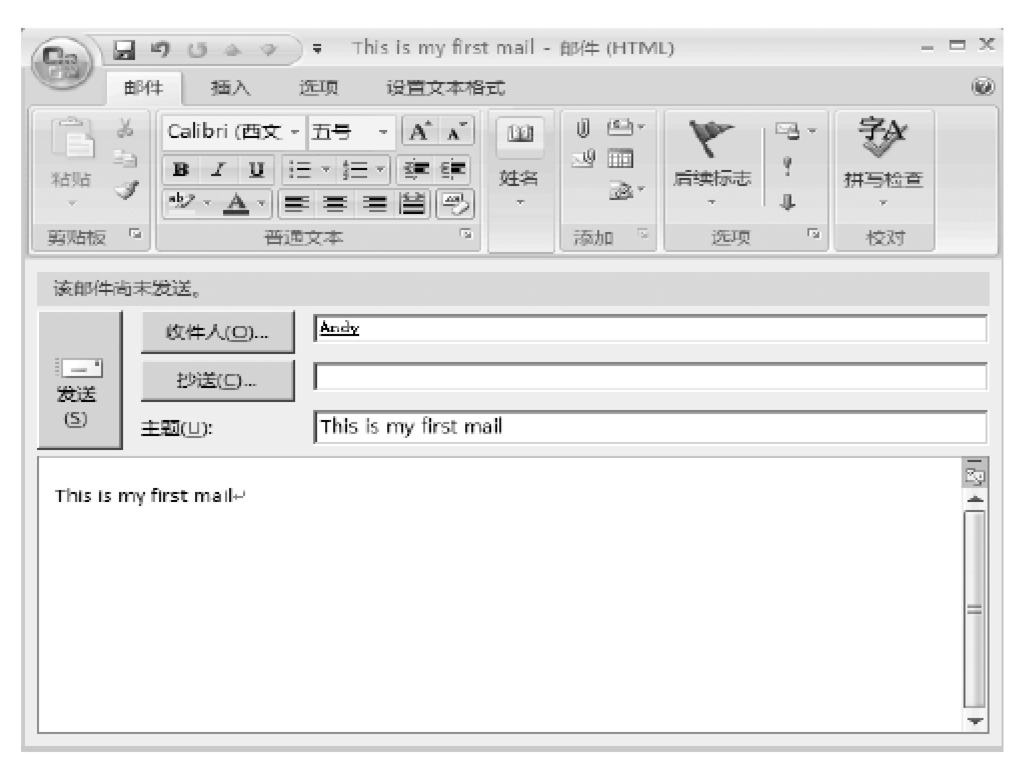


图 10-59　邮件书写窗口

(15) 下边在浏览器中以 owa 的方式登录 Andy 的邮箱，就能看到 Peter 刚刚发来的邮件，如图 10-60 所示。

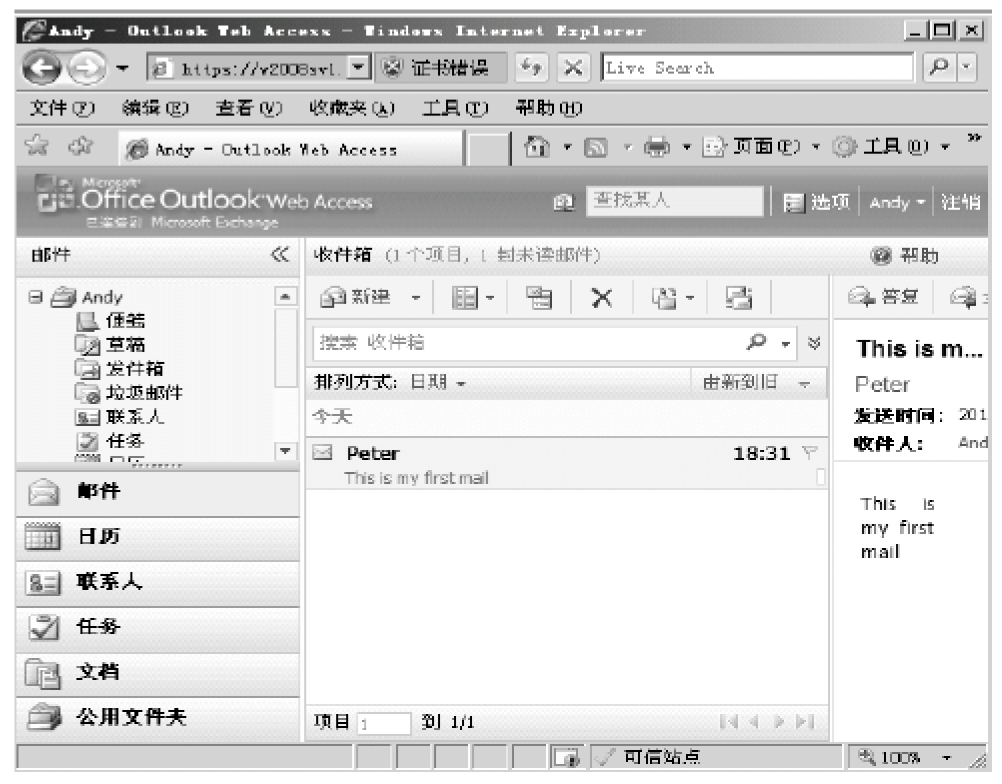


图 10-60　Andy 的邮箱

在 Outlook 2007 中经常自动下载“脱机通讯簿”，可能会遇到一个错误，如图 10-61 所示。



图 10-61　下载脱机通讯簿出错

这一错误是由于服务器设置不当引起的，解决方法如下：

在 Exchange 服务器上打开“Exchange 管理控制台”，展开“服务器配置”，选择“邮箱”。在中间的窗格中右击“Mailbox Database”，在弹出的快捷菜单中选择“属性”命令，如图 10-62 所示。

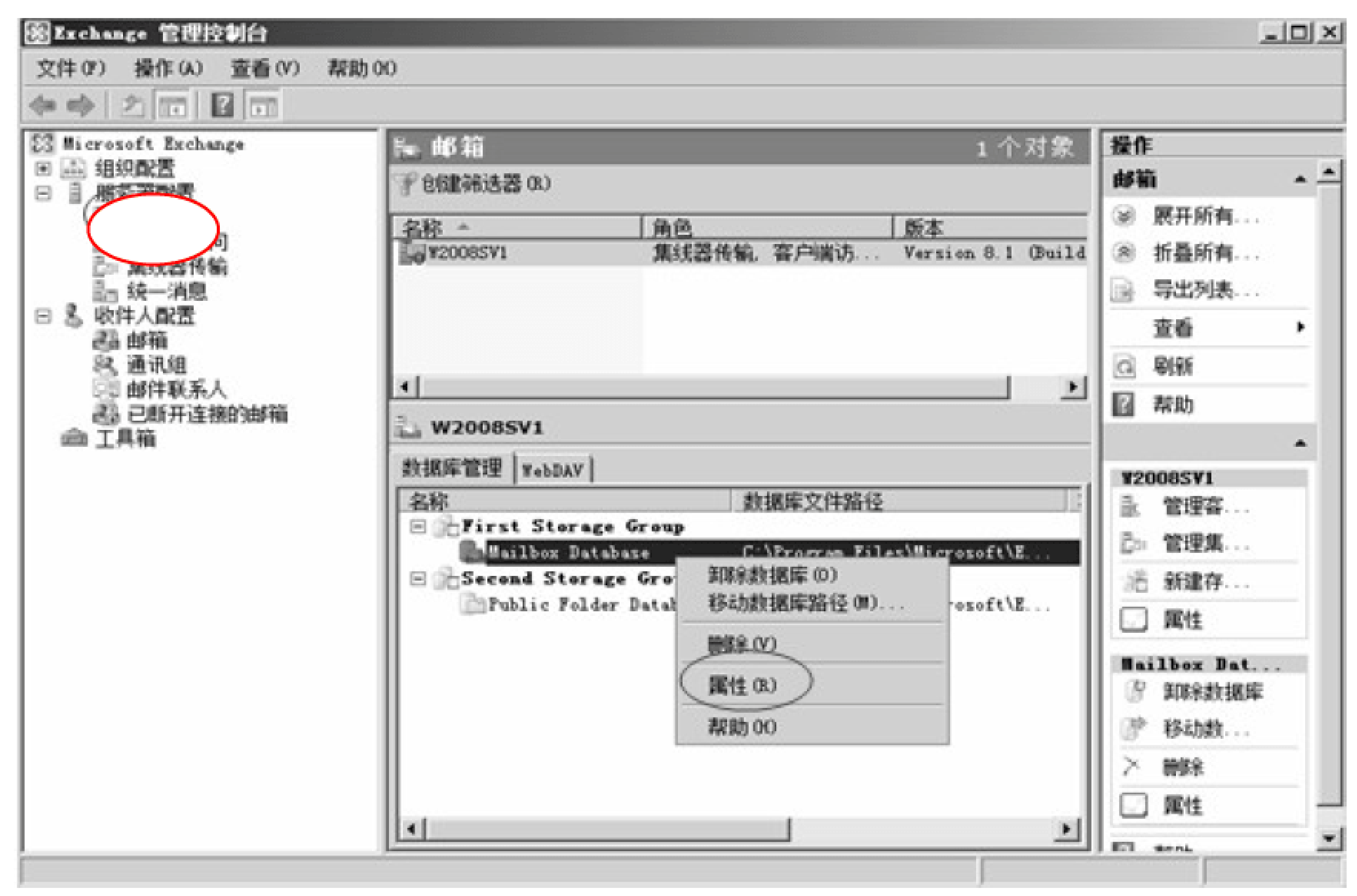


图 10-62　“Exchange 管理控制台”窗口

在接下来显示的“Mailbox Database 属性”对话框中，打开“客户端设置”选项卡，单击脱机通讯簿的“浏览”按钮，如图 10-63 所示。



图 10-63　“Mailbox Database 属性”对话框

在接下来显示的“选择脱机通讯簿”对话框中，选择“默认脱机通讯簿”，单击“确定”按钮，如图 10-64 所示。



图 10-64　“选择脱机通讯簿”对话框

接下来返回“Mailbox Database 属性”对话框，单击“确定”按钮，如图 10-65 所示。



图 10-65　“Mailbox Database 属性”对话框

下面在“Exchange 管理控制台”中，展开“组织配置”，选择“邮箱”，在中间的窗格中打开“脱机通讯簿”选项卡，右击“默认脱机通讯簿”，在弹出的快捷菜单中选择“更新”命令，如图 10-66 所示。



图 10-66　更新默认脱机通讯簿

在接下来显示的询问对话框中单击“是”按钮，如图 10-67 所示。

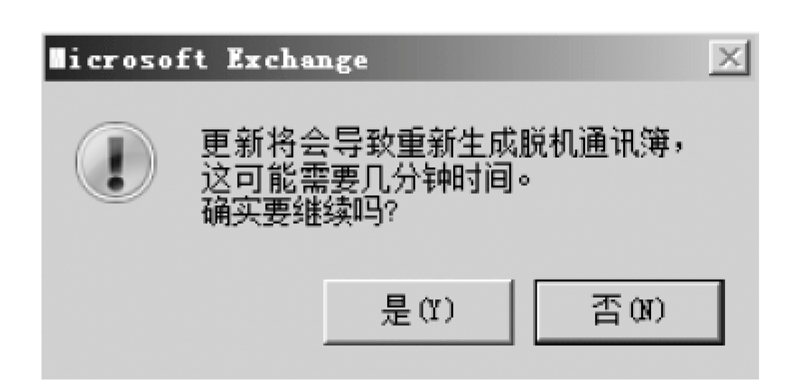


图 10-67　询问对话框

这一步的作用是产生或更新“默认脱机通讯簿”，但是“默认脱机通讯簿”还没有发布到 Web 站点。如果要立刻发布，可以在“Exchange 命令行管理程序”中执行以下命令：

Update-filedistributionservice –identity　w2008sv1

如图 10-68 所示。

这样就可以解决下载“脱机通讯簿”时出现的错误了。

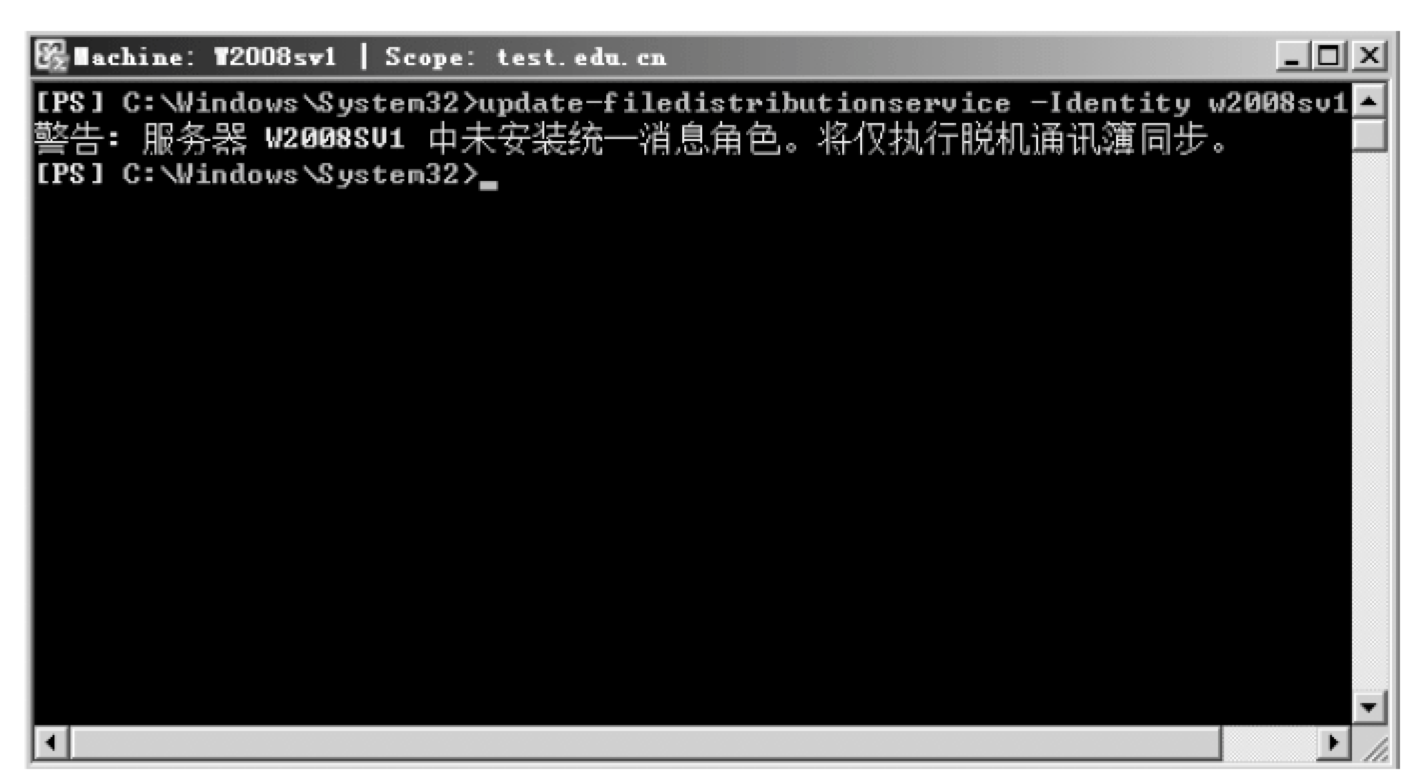


图 10-68　Exchange 命令行管理程序

10.5　配置集线器传输服务器

配置面向 Internet 的集线器传输服务器的步骤如下：

以 Administrator 的身份登录域，打开“Exchange 管理控制台”，展开“组织配置”，单击“集线器传输”，在中间的窗格中打开“接受域”选项卡，能够看到 test.edu.cn 这一接受域。这一服务器上邮箱地址的后缀到现在为止都是@test.edu.cn，例如 Andy@test.eud.cn、Peter@test.edu.cn 等，就是因为有这样一个接受域，如图 10-69 所示。



图 10-69　“Exchange 管理控制台”窗口

当 Internet 上的某一邮件服务器向 Peter@test.edu.cn 发一封邮件时，它怎样才能找到 Peter 所在的 Exchange 服务器呢？这就要求此 Exchange 服务器在 Internet 上具有可用的 IP 地址，在公用域名系统(DNS)服务器上有解析该地址的 A 类型记录，并且注册了接受域 test.edu.cn 的 MX 资源记录，如图 10-70 所示，这里仅是在内部 DNS 上的一个演示，并非真正公用域名系统(DNS)服务器中的内容。

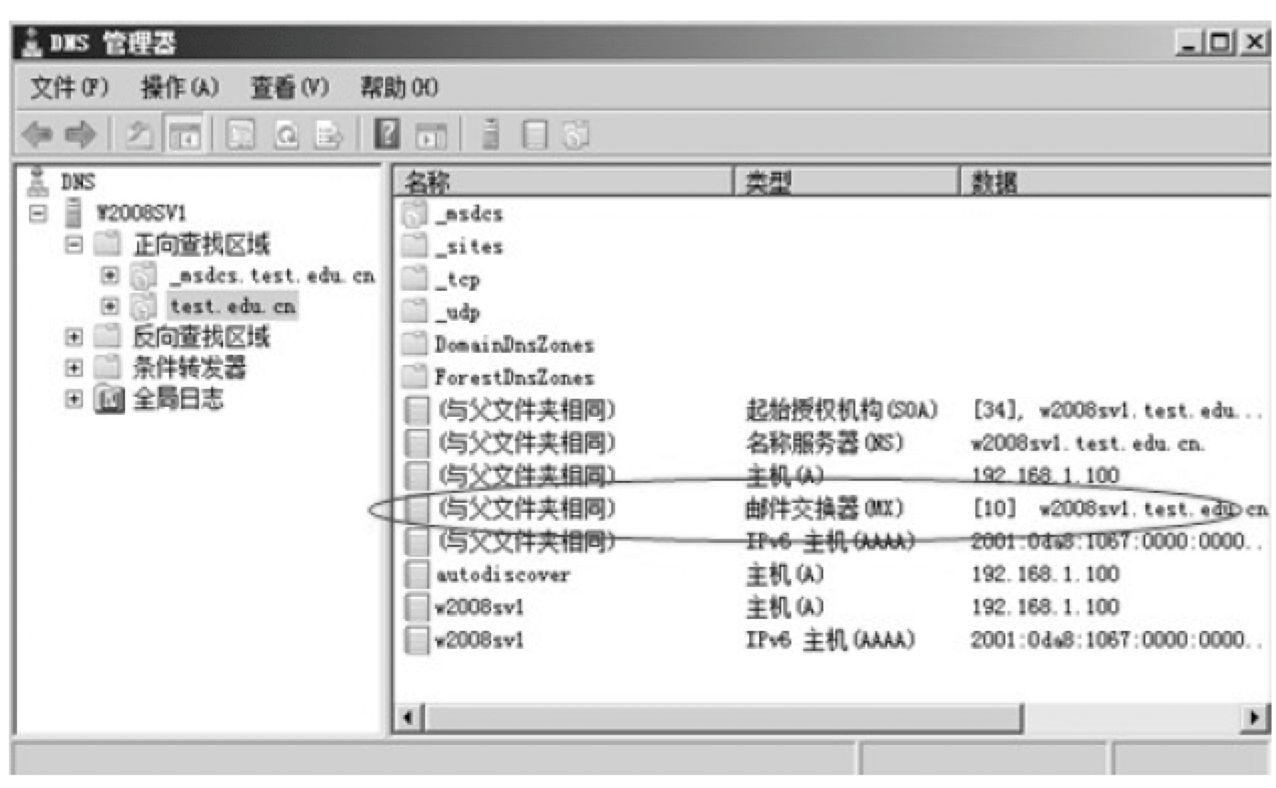


图 10-70　“DNS 管理器”窗口

由于安全原因，默认情况下，集线器传输服务器不能直接面对 Internet 收发邮件，需

要经过边缘传输服务器才能与 Internet 交换邮件。本章的操作环境中不安装边缘传输服务器角色，所以必须对集线器传输服务器进行配置才能使 Exchange 服务器与 Internet 交换邮件。配置步骤如下：

(1) 打开“Exchange 管理控制台”，展开“组织配置”，单击“集线器传输”，打开“发送连接器”选项卡，然后在操作窗格中单击“新建发送连接器”，如图 10-71 所示。



图 10-71　单击“新建发送连接器”

(2) 接下来出现“新建 SMTP 发送连接器”向导的“简介”界面，在“名称”文本框中输入连接器的唯一名称，这里输入 Internet connector。从“选择此连接器的预期用法”下拉列表中，选择 Internet 选项，然后单击“下一步”按钮，如图 10-72 所示。



图 10-72　指定发送连接器名称和用法

(3) 在“地址空间”界面中，单击“添加”按钮，如图 10-73 所示。



图 10-73　地址空间对话框

(4) 在“SMTP 地址空间”对话框中，输入“*”，然后单击“下一步”按钮，如图 10-74 所示。



图 10-74　“SMTP 地址空间”对话框

返回“地址空间”界面，如图 10-75 所示，然后单击“下一步”按钮。

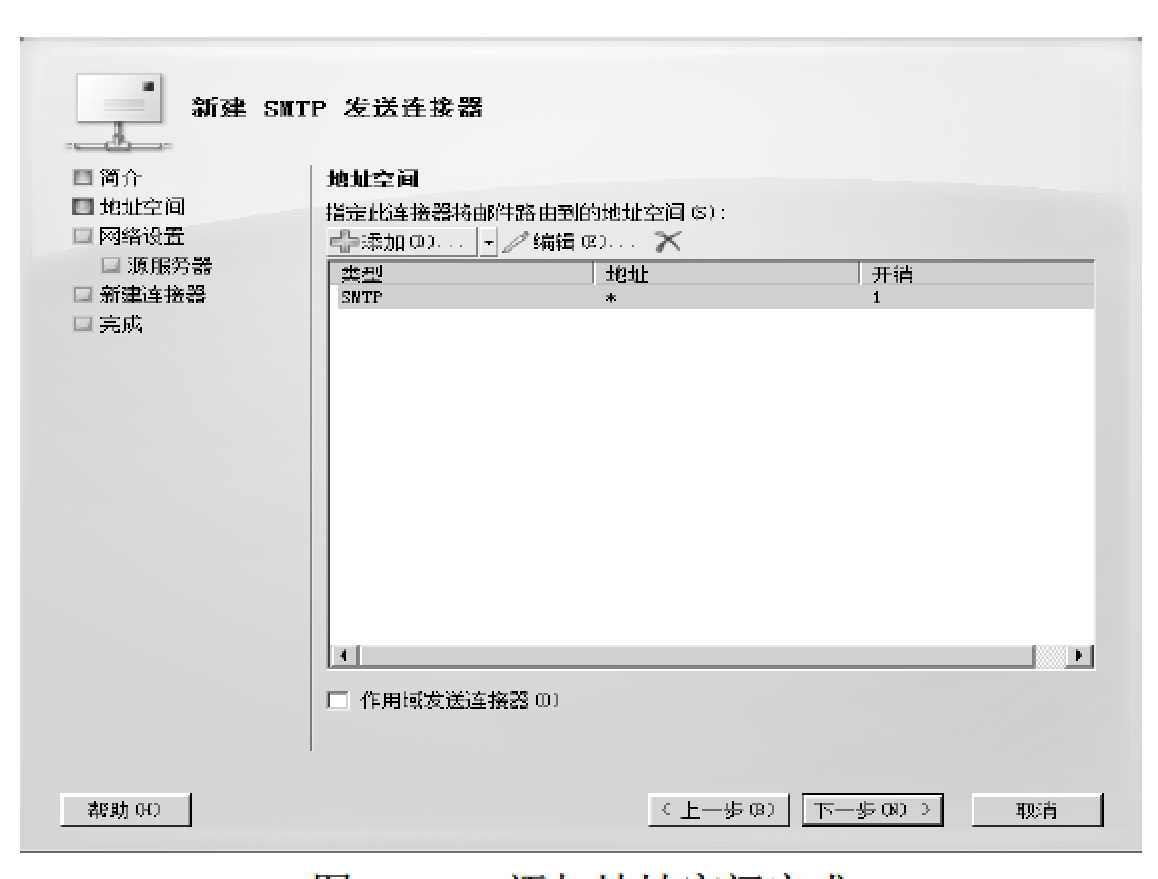


图 10-75　添加地址空间完成

(5) 在“网络设置”界面中，选择“使用域名系统(DNS)自动路由邮件”，如图 10-76 所示。

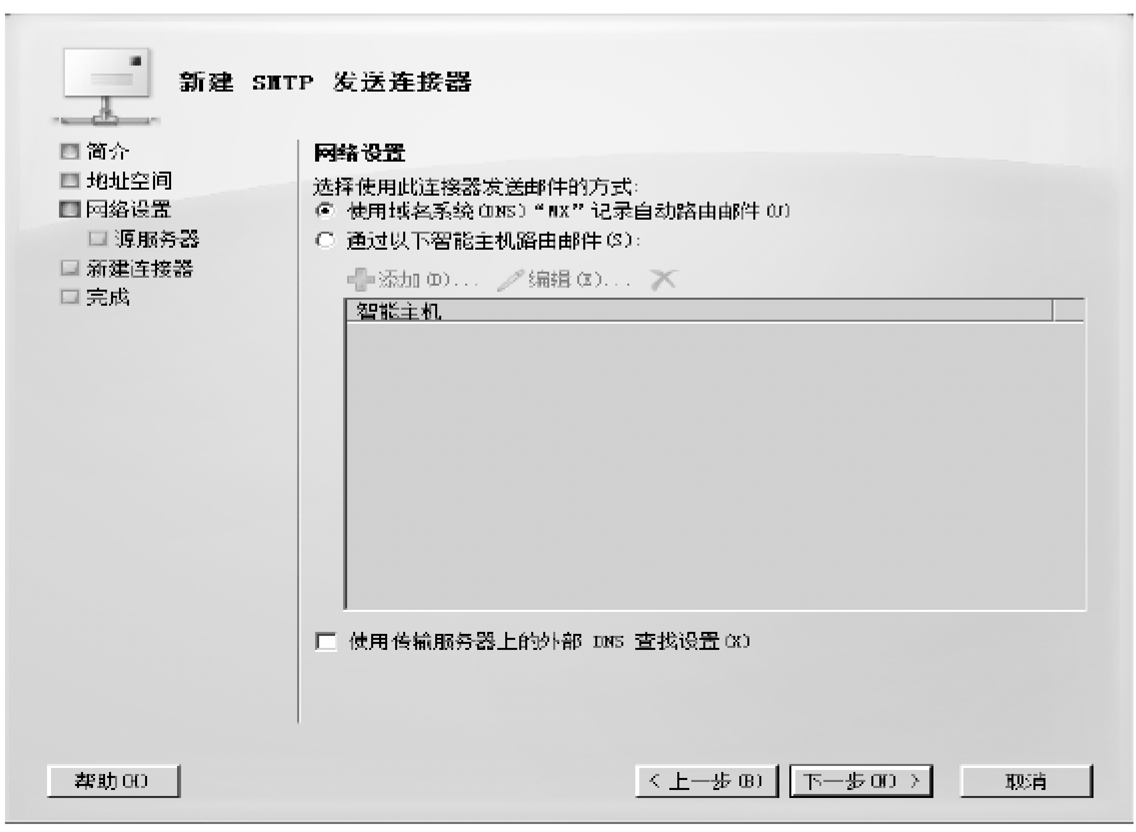


图 10-76　选择发送邮件的方式

(6) 单击“下一步”按钮，在“源服务器”界面中，选择组织中的一台或多台集线器传输服务器，然后单击“下一步”按钮，如图 10-77 所示。



图 10-77　指定源服务器

(7) 在“新建连接器”界面中，单击“新建”按钮，如图 10-78 所示。



图 10-78　查看新建连接器配置摘要

(8) 在“完成”界面中单击“完成”按钮，如图 10-79 所示。

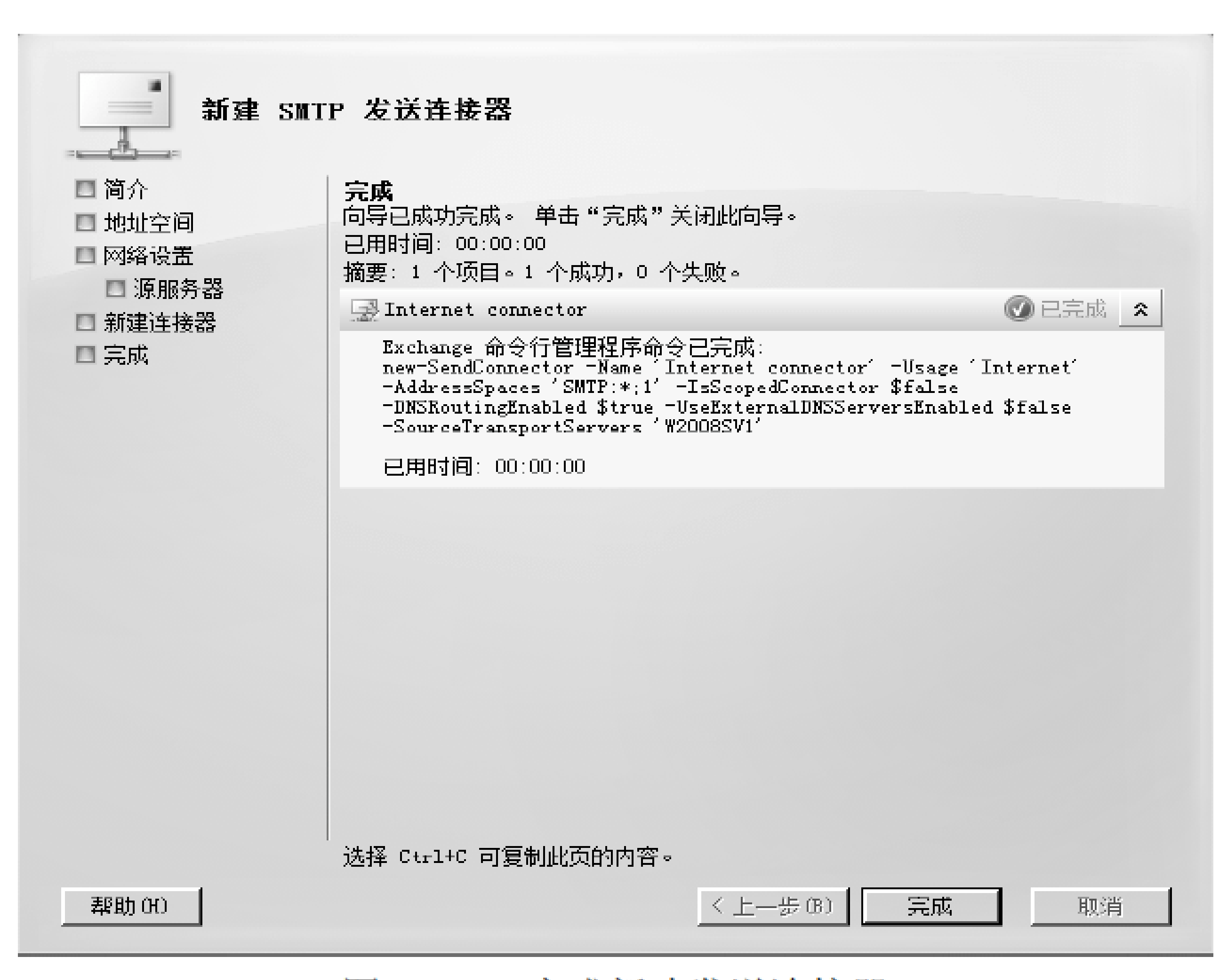


图 10-79　完成新建发送连接器

以上是新建发送连接器，目的是向 Internet 发送邮件。以下是修改默认接收连接器，以允许匿名连接，目的是接收来自 Internet 的邮件。

(9) 返回“Exchange 管理控制台”窗口后，展开“服务器配置”，单击“集线器传输”，然后在“接收连接器”选项卡下面的工作窗格中，选择“Default w2008sv1”连接器。在操作窗格中，单击“属性”链接，如图 10-80 所示。



图 10-80　设置 Default w2008sv1 连接器的属性

(10) 在“Default w2008sv1 属性”对话框中，打开“权限组”选项卡，选择“匿名用户”，允许匿名用户连接到此接收连接器，单击“确定”按钮，如图 10-81 所示。

通过上述配置，在不安装边缘传输服务器角色的情况下，Exchange 服务器也能与 Internet 交换邮件。



图 10-81　允许匿名用户连接

10.6　邮箱常用操作和限制

10.6.1　邮箱空间的限制

每个邮箱都要占用服务器硬盘的磁盘空间，如果不对邮箱所占空间进行限制，很快服务器的磁盘空间就会用尽。因此，对邮箱空间进行限制，是电子邮件服务器的基本功能。下边介绍如何进行邮箱空间的限制。

打开“Exchange 管理控制台”，展开“服务器配置”，单击“邮箱”，在中间的窗格中打开“数据库管理”选项卡，单击“MailBox Database”，在操作窗格中单击“属性”链接，如图 10-82 所示。



图 10-82　“Exchange 管理控制台”窗口

在“Mailbox Database 属性”对话框中，打开“限制”选项卡，从中可以看到“存储限制”，对邮箱空间的限制可以在此设置，此数据库中的所有邮箱，默认情况下都受该存储限制的约束，如图 10-83 所示。

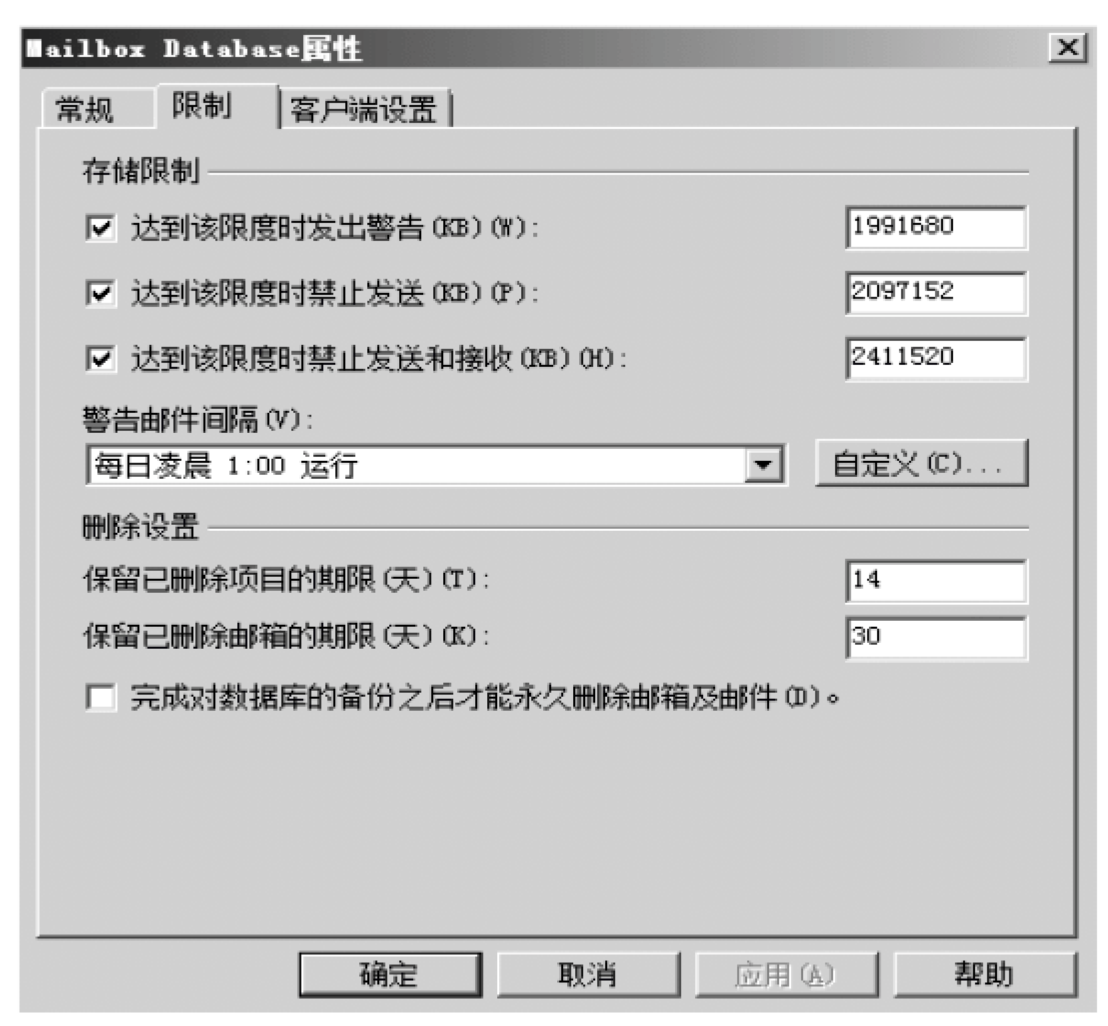


图 10-83　整体限制邮箱空间

要限制个别邮箱的空间，可以执行下面的操作：

打开“Exchange 管理控制台”，展开“收件人配置”，单击“邮箱”，在中间的窗格中单击选择要限制空间的邮箱所对应的名称，这里单击选择“Andy”，在操作窗格中单击“属性”，如图 10-84 所示。



图 10-84　选择 Andy 的属性

在“Andy 属性”对话框中打开“邮箱设置”选项卡，单击“存储配额”，然后单击“属性”，如图 10-85 所示。



图 10-85　选择存储配额的属性

在“存储配额”对话框中，只要取消了存储配额下的“使用邮箱数据库默认值”复选框，就可以对当前邮箱的空间进行限制了，如图 10-86 所示。

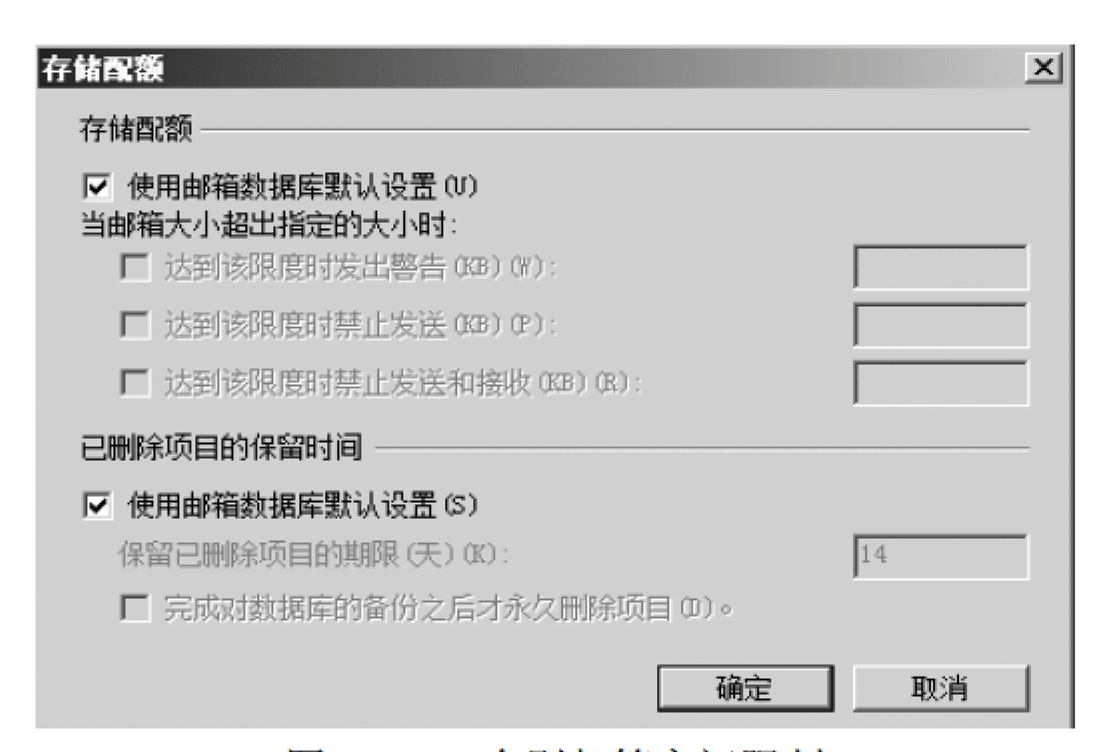


图 10-86　个别邮箱空间限制

10.6.2　邮箱的管理

邮箱的管理包括对邮箱的禁用、删除与恢复。

在电子邮件服务器上除了建立邮箱，还需要经常删除不用的邮箱，除此之外 Exchange Server 还提供了禁用和恢复邮箱功能，下边通过具体实例来介绍这些功能的使用。

如果在操作窗格中不单击“属性”，而单击“禁用”，则会弹出“警告”对话框，如图 10-87 所示，在此单击“是”按钮，则 Andy 邮箱就被禁用，不能再使用了。但邮箱并没有真正消失，默认情况下，30 天之内都能被恢复。



图 10-87　禁用邮箱警告

如果要恢复该邮箱，就展开“收件人配置”，单击“已断开连接的邮箱”，在中间窗格中能看到断开连接的邮箱“Andy”，单击“Andy”，并在操作窗格中单击“连接”，如图 10-88 所示。



图 10-88　单击“连接”

在“连接邮箱”对话框的“简介”界面中，选择“用户邮箱”，单击“下一步”按钮，如图 10-89 所示。

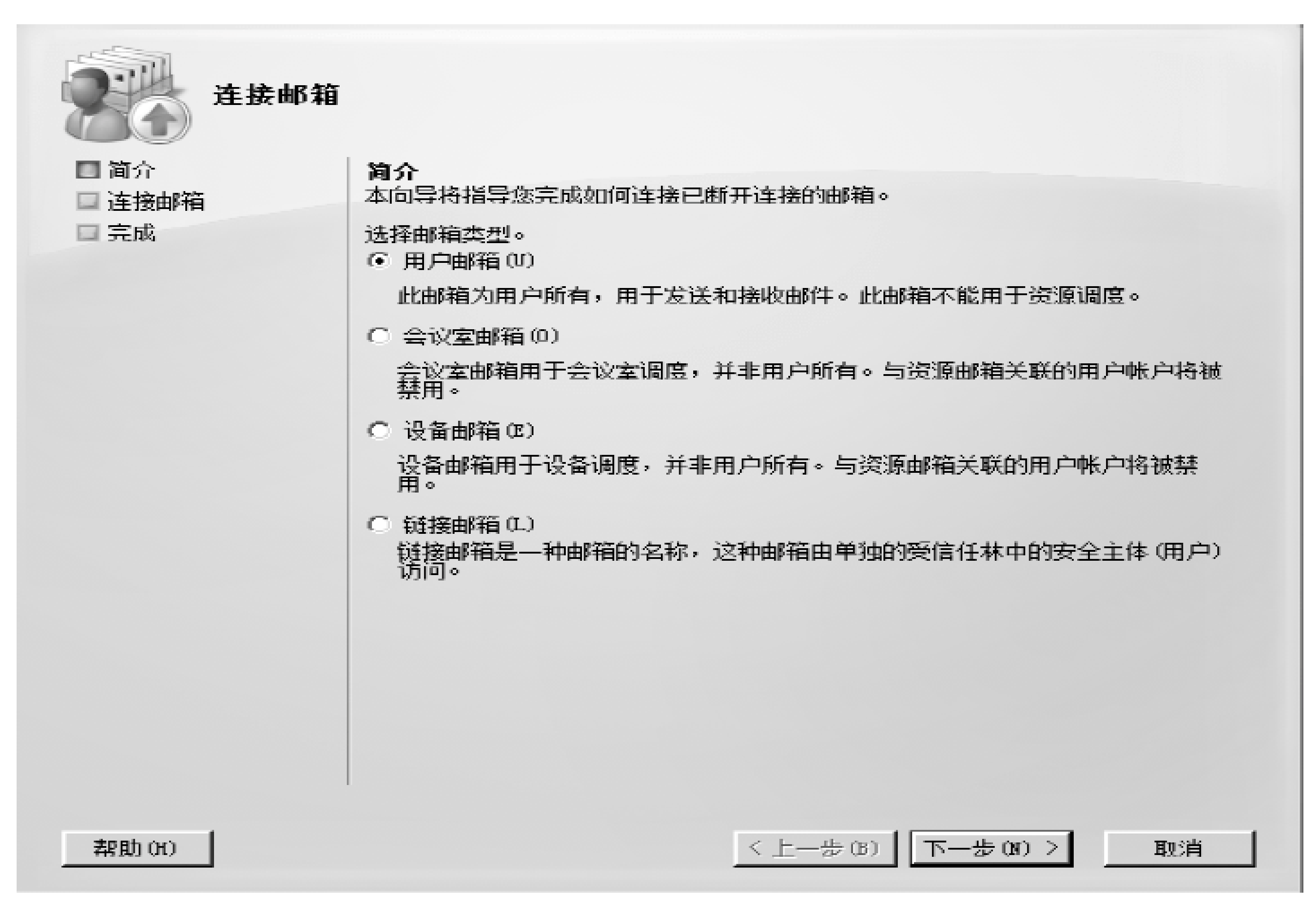


图 10-89　选择用户邮箱

在“邮箱设置”对话框中选择“匹配用户”，单击“浏览”按钮，如图 10-90 所示。

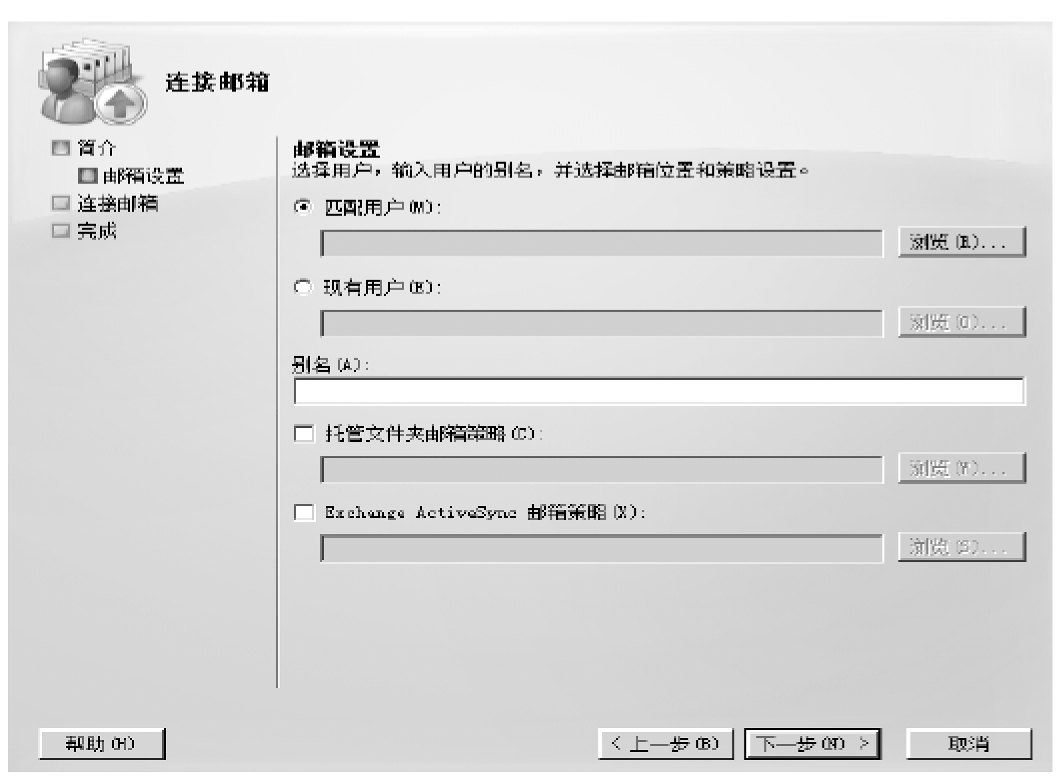


图 10-90　择匹配用户

在“选择用户”对话框中，选择“Andy”，然后单击“确定”按钮，如图 10-91 所示。



图 10-91　选择 Andy 用户

返回“邮箱设置”对话框后，单击“下一步”按钮。在“配置摘要”界面中单击“连接”按钮，如图 10-92 所示。

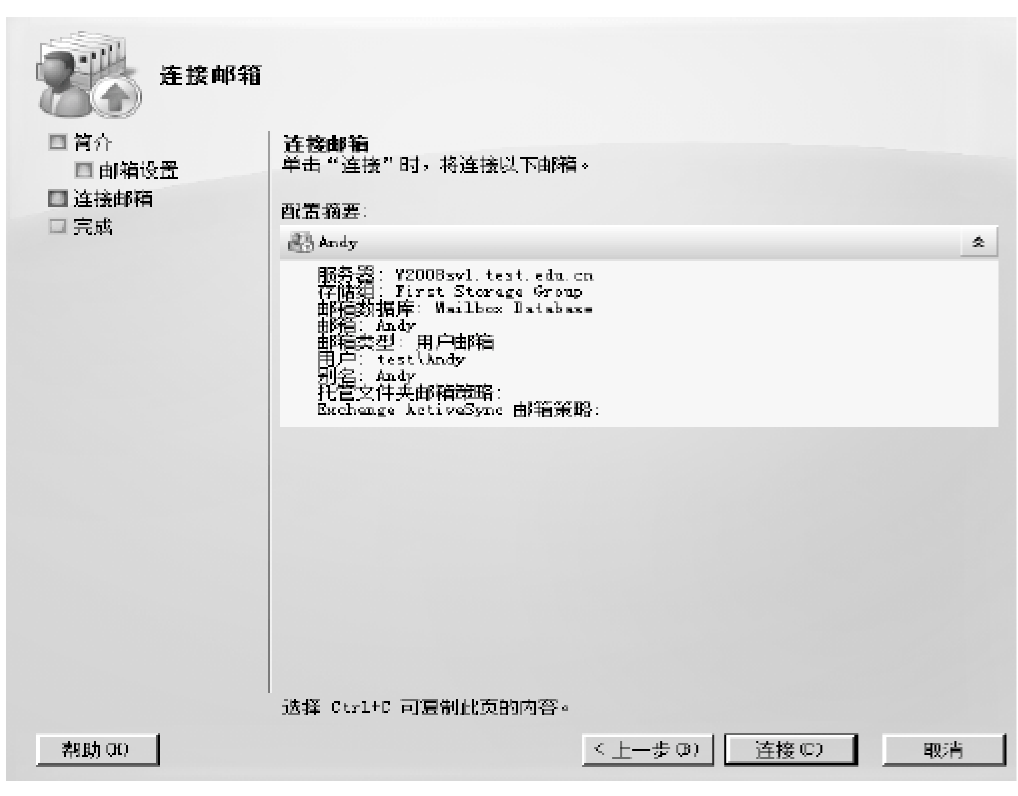


图 10-92　连接禁用的邮箱

然后在“完成”界面中，单击“完成”按钮，最后完成 Andy 邮箱的恢复。

如图 10-93 所示，如果在操作窗格中不单击“属性”，而单击“删除”，则会弹出“警告”对话框，在“警告”对话框中单击“是”按钮，则 Andy 邮箱就被删除。但邮箱同样并没有真正消失，默认情况下，30 天之内也可以被恢复。

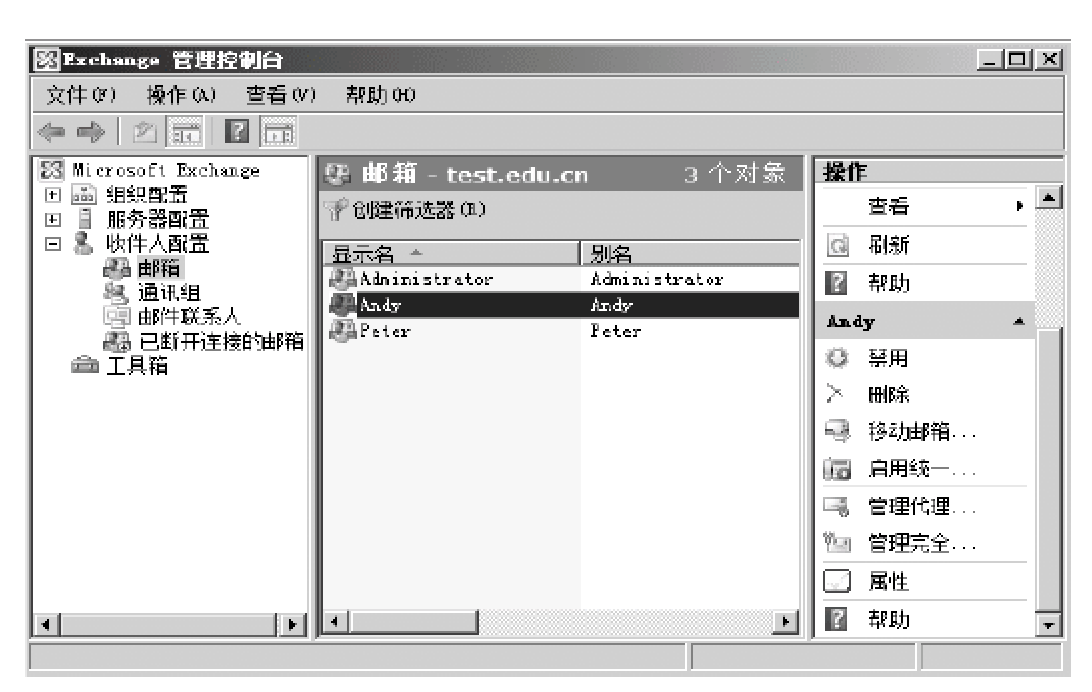


图 10-93　删除邮箱

删除邮箱与禁用邮箱不同，禁用邮箱时邮箱对应的域用户不会被删除，但删除邮箱时邮箱对应的域用户将被删除，打开“Active Directory 用户和计算机”就会发现被删除邮箱对应的域用户也被删除了。因此恢复被删除的邮箱前需要先建一个域用户。比如删除 Andy 邮箱后，在恢复之前最好在“Active Directory 用户和计算机”中再建一个名为 Andy 的域用户，后面的恢复步骤就与恢复被禁用的邮箱一样了。

10.7　本章小结

Exchange Server 2007 是一个功能强大的电子邮件系统和企业信息平台，本章只是简单介绍了系统的安装、邮箱的基本操作(建立、空间限制、禁用、删除和恢复)、客户端使用 Outlook 或 OWA 进行邮件的收发、配置集线器传输服务器直接面向 Internet(虽然这样不够安全，但完全可以面对 Internet 收发邮件)几个方面，不过这些配置已经完全可以构建一个简单可用的邮件系统了。

10.8　思考与练习

【思考题】

1. Exchange Server 2007 中的服务器角色分为几类？分别是哪几类？
2. 设置边缘传输服务器角色的作用是什么？
3. 安装 Exchange Server 2007 之前，需要添加什么服务?安装哪些软件？

【练习题】

建立两个邮箱，一个是 Tom 一个是 Jerry，分别用 OWA 和 Outlook 互发邮件。

第11章　流媒体服务

【本章导读】

随着 Internet 的发展，各种网络的带宽都在不断增加，网络视频服务逐渐兴起，各种视频网站、播客服务如雨后春笋般出现，在一定程度上改变了人们的生活习惯。网络视频服务具有传输速率高、稳定性好的特性，广泛用于电子商务、新闻发布、网络广告、视频直播、影视直播、远程教育、远程医疗和视频会议等多个服务领域。支撑网络视频服务蓬勃发展的技术就是流媒体技术。微软公司也开发了流媒体技术。微软的流媒体技术是基于其自身的 Windows Media 多媒体技术，同时充分利用了 Windows Media Player 和 IE 浏览器的技术，使 Windows Media 技术在流媒体市场上拥有一席之地。Windows Server 2008 能够良好支持这些技术，使用户能够方便地在网络上发布视频信息。

11.1　流媒体服务的安装

11.1.1　流媒体概述

网络上传输音视频主要有两种方法，一是非实时方式，这种方式要求用户将整个媒体文件下载到本地磁盘，再使用一定的播放软件打开，这种方式媒体质量较高，但是带宽占用高，如果不全部下载还不能观看；另一种是实时方式，也就是采用流媒体技术的方式，这种方式允许用户将媒体文件下载一小部分到本地磁盘，并且直接播放，实现边下载边播放，使用上更加方便，但是受网络带宽影响，影音质量可能会较差。

常见的流媒体技术有Microsoft公司的Windows Media，RealNetworks公司的RealSystem，Apple 公司的 QuickTime 等。

11.1.2　流媒体传输协议

Windows Server 2008 上的流媒体平台所采用的传输协议是 RTSP，此外还支持 HTTP 协议，而在此之前 Microsoft 公司主推的 MMS 协议逐渐淘汰。

- RTSP 协议：Real Time Streaming Protocol，实时流传输协议，是 TCP/IP 协议体系中的一个应用层协议，由哥伦比亚大学、网景和 Real Networks 公司共同开发，使用 554 端口。该协议定义了一对多应用程序如何有效地通过 IP 网络传送多媒体数据。RTSP 在体系结构上位于 RTP 和 RTCP 之上，它使用 TCP 或 RTP 完成数据传

输。RTSP 用来控制声音或影像的多媒体串流协议，并允许同时多个串流需求控制，传输时所用的网络通信协议并不在其定义的范围内，服务器端可以自行选择使用 TCP 或 UDP 来传送串流内容，它的语法和运作跟 HTTP 类似，但并不特别强调时间同步，比较能容忍网络延迟，而且可以根据用户连接的带宽进行动态调整，用户可以从媒体的任意时间点开始观看媒体问题，因此比较适合用于网络上传输媒体文件。

- HTTP 协议：Windows Server 2008 的流媒体平台还支持 HTTP 协议。使用 HTTP 协议传输媒体文件，使用 80 端口，因此基本上不受防火墙限制，使用方便，兼容性好，音视频质量较高。但是 HTTP 协议只能顺序传输媒体文件，因此不能任意设置音视频播放的起始时间点，不能支持现场直播，而且对带宽要求较高。

11.1.3　点播与广播

流媒体播放有两种方式，分别是点播和广播。

点播是指用户主动与服务器进行连接，用户可以选择自己想看的节目，服务器响应用户的请求，将被选择节目传输给用户。在播放过程中，用户可以对播放的内容进行开始、停止、暂停、快进和快退等操作。这种方式使用户较大的自由度，但是由于每个用户和服务器之间都要建立一个单独的连接，对服务器的性能和网络带宽要求较高。

广播是指媒体服务器主动发送数据，用户被动接受媒体文件。在广播过程中，用户只能接收数据，不能对播放的内容进行暂停、快进等控制，自由度较低，但是对服务器的性能及带宽要求低于点播模式。因此广播方式常用于网络广播或现场直播。

11.1.4　流媒体服务的安装

Windows Server 2008 中配备的新一代多媒体内容发布平台 Windows Media Services 2008 可以在 32 位和 64 位的 Web 版、标准版、企业版和数据中心版的 Windows Server 2008 中进行安装。Windows Media Services 2008 的应用环境非常广泛，在企业内部应用环境中，可以实现点播方式视频培训、课程发布、广播等。在商业应用中，可以用来发布电影预告片、新闻娱乐、动态插入广告、音频视频服务等。

Windows Media Services 2008 具备以下核心功能。

1. fast steaming

这个功能在 Windows Media Services 9.0 中就已经出现，在 Windows Media Services 2008 中进行了优化。fast steaming 功能包含快速开始、快速缓存、快速连接和快速恢复等功能，从用户体验上来看，当播放一个流媒体视频，漫长的等待时间和断断续续的播放质量必然使观众观看视频的兴趣大减，而 fast steaming 功能使观众可以流畅地观看流媒体视频，并且减少缓冲等待的时间。

Windows Media Services 2008 支持多编码率视频或者音频，可以动态地检测用户带宽，

并且智能地为用户选择不同编码率的视频音频文件，从而保证流媒体文件播放的速度，增强用户体验。

2. 更多的并发连接支持

Windows Media Services 2008 通过带宽检测、智能选择编码率以及 fast steaming 等功能，大大提升了性能，从而相对以前的 Windows Media Services 版本可以支持更多的并发连接数。在相同硬件条件下，Windows Media Services 2008 每服务器并发连接用户数量可以达到以前的 2 倍。

3. Serve Core 安装模式

从 Windows Server 2008 开始，管理员可以选择安装具有特定功能，但不包含任何不必要功能的 Server Core 最小安装模式，它为一些特定服务的正常运行提供了一个最小的环境，从而减少了其他服务和管理工具可能造成的攻击和风险。Windows Media Services 2008 支持在 Server Core 模式进行安装，从而将风险和资源占用减到最低。

4. 集成的 cache/proxy 功能

Windows Media Services 2008 集成缓存/代理功能，也是为了提高流媒体播放速度和质量而设计。举个例子来说，比如在企业应用中，可以通过 Windows Media Services 2008 来构架一台流媒体服务器，用来发布企业内部的培训视频、音频讲座等。如果同时访问服务器的用户非常多，会给服务器造成很大压力，影响视频的播放速度。这时候可以利用 Windows Media Services 2008 的 cache/proxy 功能，在本地构架一台缓存服务器，将播放的内容进行缓存，从而提高流媒体的播放速度。

5. 集成丰富的管理工具

Windows Media Services 2008 安装成功后，在 Windows Server 2008 的管理工具中生成一个控制台，并且用户也可以通过 Server Manager 工具来进行管理，同时，Windows Media Services 2008 和 IIS 紧密结合，支持远程管理功能。

归结起来，Windows Media Services 2008 相对以前的版本具有三大改进：

(1) 增强的流媒体性能和用户体验。fast streaming 技术，动态带宽检测，多编码率支持，支持 RTSP、HTTP、IGMPv3、IPv6 等多种协议，并且针对无线连接进行优化。

(2) 动态内容编辑。Windows Media Services 2008 中还有一个非常有意思的功能就是支持动态内容编辑，可以在播放过程中动态调整播放的内容，如根据不同的用户群体播放不同视频内容、插播广告等。并且可以根据不同用户的带宽选择不同编码率，从而提高播放速度。

(3) 业界领先的媒体平台。Windows Media Services 2008 支持二次开发，用户可以根据需求自定义高级内容。

和以前版本的 Windows Server 系统不同，Windows Server 2008 是不自带流媒体服务器软件的，需要从 Microsoft 公司网站上下载相应的升级包才能安装。步骤如下：

(1) 管理员打开网页 http://www.microsoft.com/downloads/zh-cn/details.aspx?FamilyID=9ccf6312-723b-4577-be58-7caab2e1c5b7，如图 11-1 所示。

此下载的文件

本节中的链接对应此下载包含的各个文件。下载文件最适合你文件。

文件名：	下载大小：	下载下列文件
Windows6.0-KB934518-x64-Admin.msu	9.0 MB	下载
Windows6.0-KB934518-x64-Core.msu	10.8 MB	下载
Windows6.0-KB934518-x64-Server.msu	20.2 MB	下载
Windows6.0-KB934518-x86-Admin.msu	8.7 MB	下载
Windows6.0-KB934518-x86-Core.msu	10.5 MB	下载
Windows6.0-KB934518-x86-Server.msu	19.7 MB	下载

图 11-1　下载页面

(2) 网页中共有两组共 6 个下载项，其中标注有 X64 的项目是为 64 为 Windows Server 2008 设计的，标注有 X86 的项目是为 32 位 Windows Server 2008 设计的；标注有 Server 的项目就是需要下载的软件包，标注有 Core 的项目适用于 Core 模式安装的 Windows Server 2008，标注有 Admin 的项目则是 Windows Media Services 2008 的管理工具，可酌情下载。

本书使用的是 32 位的 Windows Media Services 2008，因此下载的项目是 Windows6.0-KB934518-x86-Server.msu。

(3) 下载完成后，双击下载文件即可开始安装，安装之前会提示需要安装更新，按照提示安装即可。安装界面如图 11-2 所示。

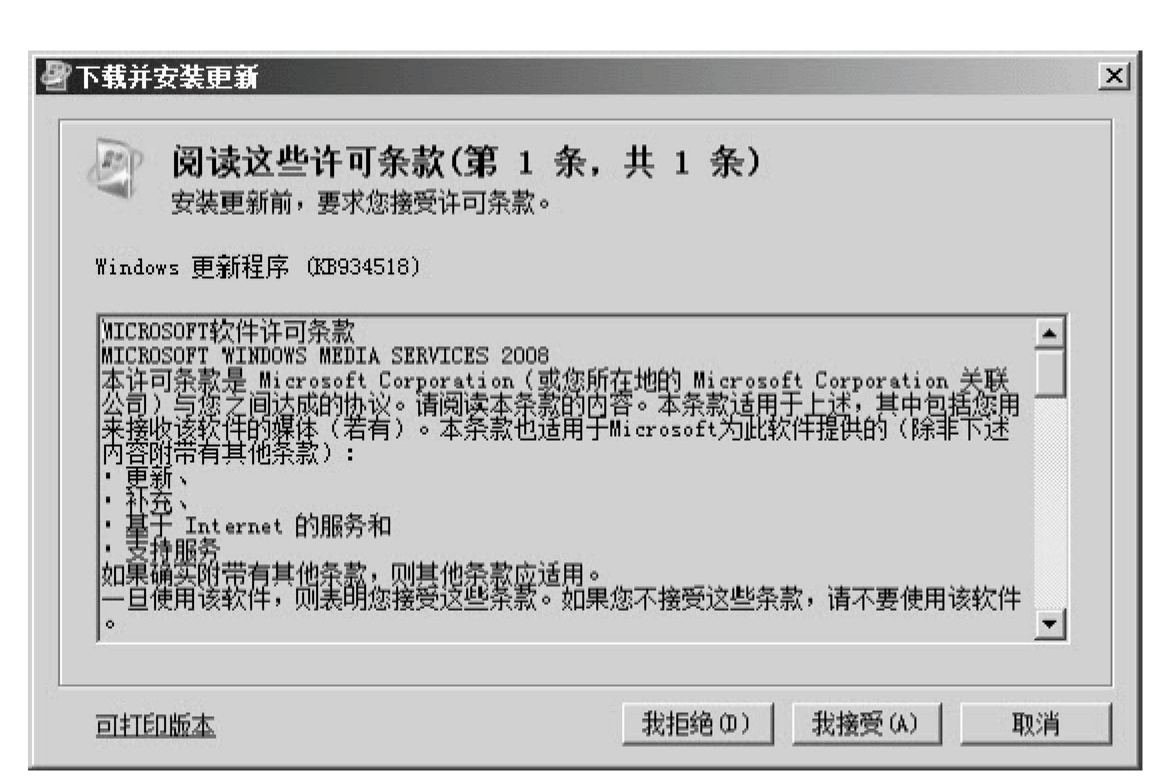


图 11-2　安装许可界面

(4) 单击“我接受”按钮，即可开始自动安装。安装完毕后，系统中不会出现任何变化，此时需要在服务器管理器中手动添加相应的角色。

(5) 选择“开始”→“管理工具”→“服务器管理器”命令，打开服务器管理器，选择“操作”→“刷新”命令，然后选择“操作”→“添加角色”命令，打开“添加角色向导”，如图 11-3 所示。



图 11-3　“选择服务器角色”界面

(6) 在向导中选择“流媒体服务”，单击“下一步”按钮，进入“流媒体服务简介”界面，再单击“下一步”按钮，选择为流媒体服务安装的角色服务，如图 11-4 所示。



图 11-4　“选择角色服务”界面

(7) 采用默认设置即可，如果需要通过网页进行流媒体服务器的管理，可以选中“基于 Web 的管理”，但需要安装 IIS 的重定向组件。选择完毕后，单击“下一步”按钮，进入“选择数据传输协议”界面，选择传输流媒体数据时使用的协议，默认采用 RTSP 协议，也可采用 HTTP 协议，但是如果同一个服务器上安装了 IIS 和流媒体服务两种服务，HTTP 协议不可选，因为 IIS 已经占用了 HTTP 的 80 端口。如图 11-5 所示。



图 11-5　“选择数据传输协议”界面

(8) 单击“下一步”按钮，进入“Web 服务器简介”界面，再单击“下一步”按钮，进入 IIS 服务器“选择角色服务”界面，如图 11-6 所示。

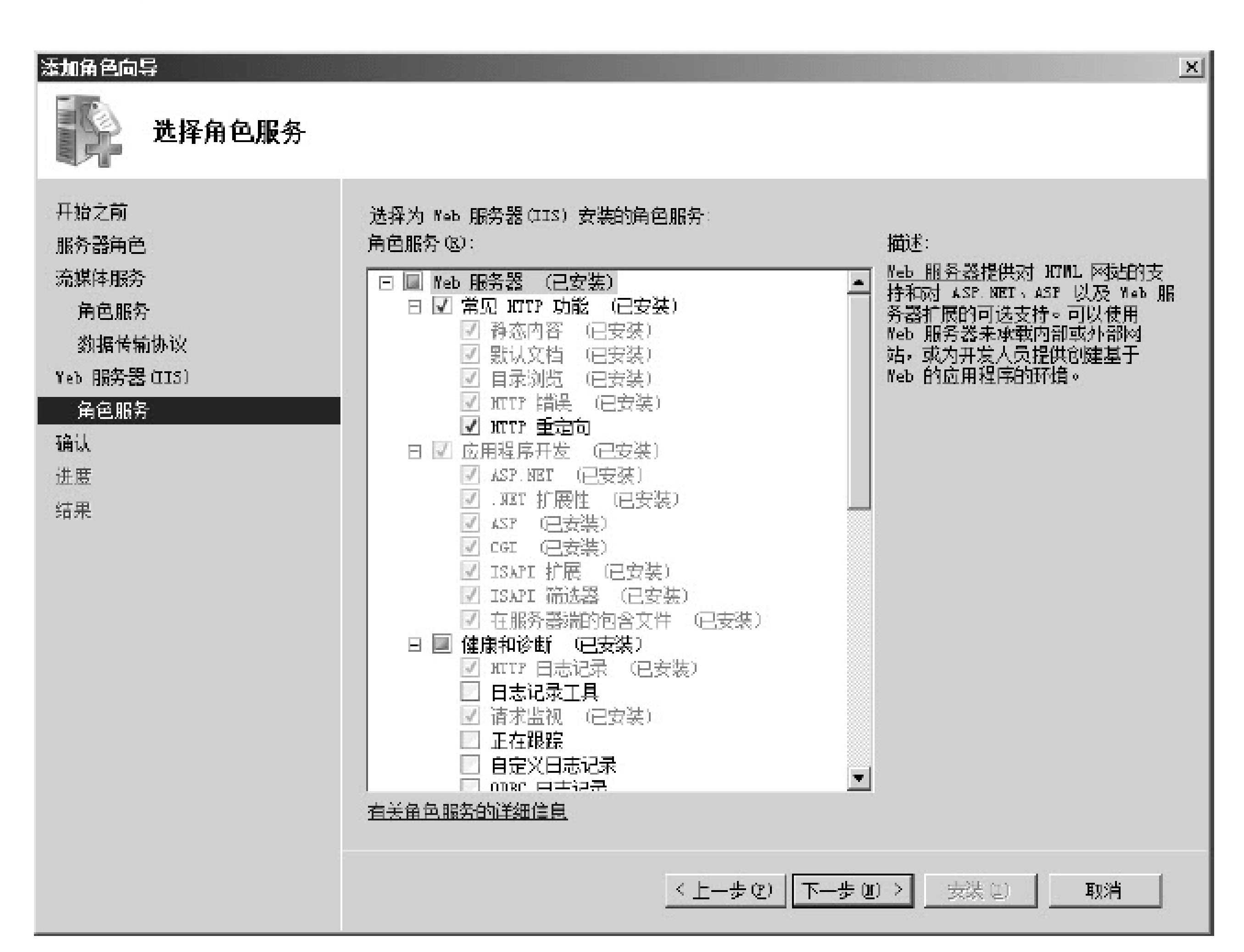


图 11-6　IIS 服务器“选择角色服务”界面

(9) 如果不需要添加服务角色，单击“下一步”按钮，进入“确认”界面，如果还有需要修改的设置，单击“上一步”按钮返回，否则，单击“安装”按钮，根据提示完成安装即可。

安装好流媒体服务器后，在配置过程中会需要在当前服务器上测试流媒体服务，这就需要在 Windows Server 2008 上安装 Windows Media Player。操作步骤如下：

(1) 打开服务器管理器，依次选择“工具”→“添加功能”命令，打开添加功能向导，

选中“桌面体验”复选框，如图 11-7 所示。

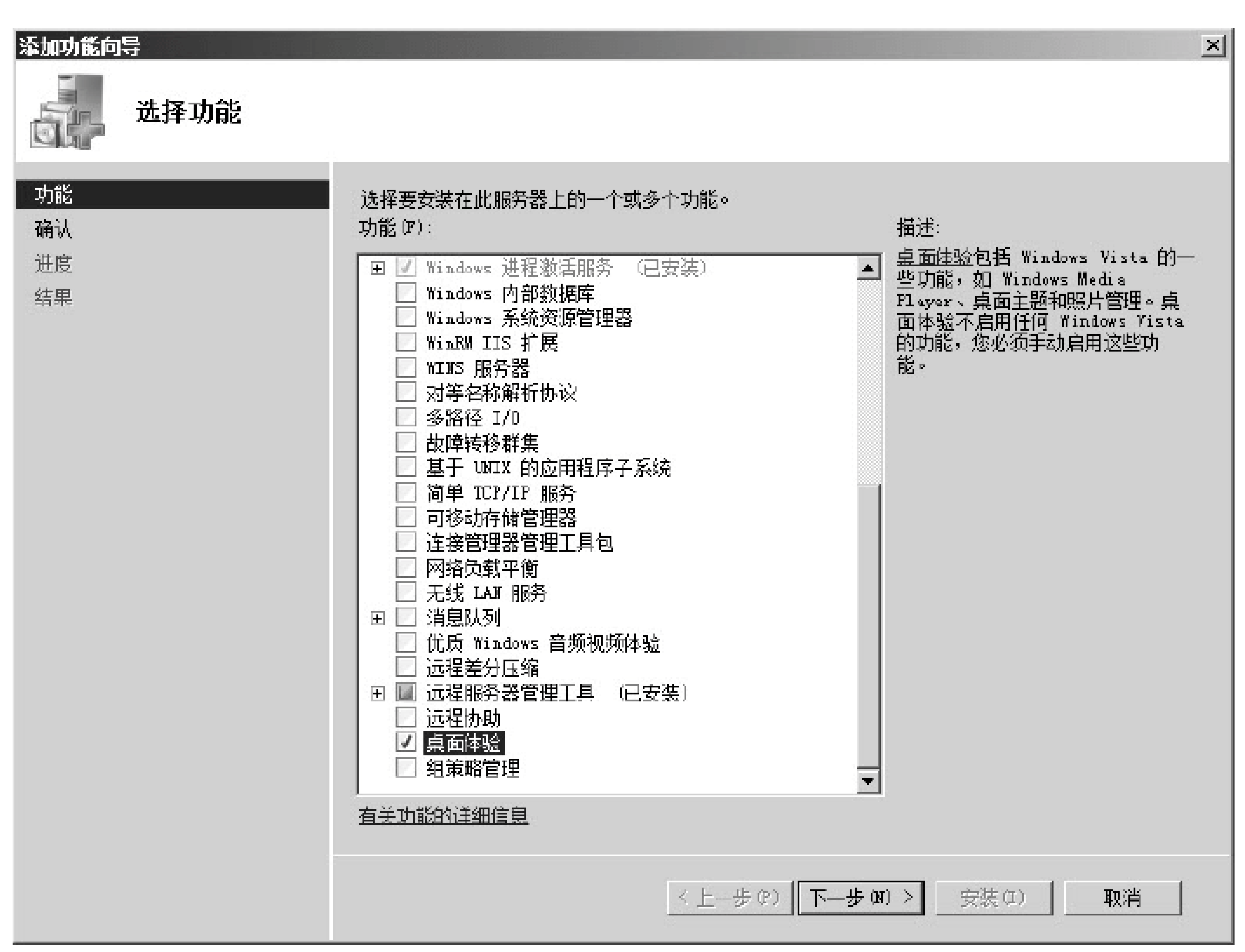


图 11-7　“选择功能”界面

(2) 单击“下一步”按钮，进入“确认安装”界面，如果还需要安装其他功能，可单击“上一步”按钮返回以便更改，如果不需要更改安装设置，则单击“安装”按钮开始安装，如图 11-8 所示。



图 11-8　“安装进度”界面

(3) 安装完毕后，打开“安装结果”界面，如图 11-9 所示。单击“关闭”按钮，然后重启服务器即可自动完成安装。



图 11-9　“安装结果”界面

11.2　实现点播和广播

安装好流媒体服务组件后，就可以着手准备搭建流媒体站点了。首先要准备的就是流媒体文件，即支持流媒体协议的多媒体文件。Windows Media Services 2008 支持的标准文件格式为.asf、.wma、.wmv，即使当前没有这类文件，也可以使用 Windows Media 编码器，将文件扩展名为.wma、.wmv、.asf、.avi、.wav、.mpg、.mp3、.bmp 和.jpg 等多媒体文件转换成为 Windows Media 服务使用的流文件。

11.2.1　实现视频和音频点播

准备好实施点播的音视频文件后，就可以创建点播站点了。

(1) 依次选择“开始”→“管理工具”→“Windows Media 服务”命令，打开“Windows Media 服务”窗口，如图 11-10 所示。



图 11-10　“Windows Media 服务”窗口

(2) 展开窗口左侧的目录树，右击“发布点”，从弹出的快捷菜单中选择“添加发布点(向导)”命令，打开“添加发布点向导”对话框，如图 11-11 所示。

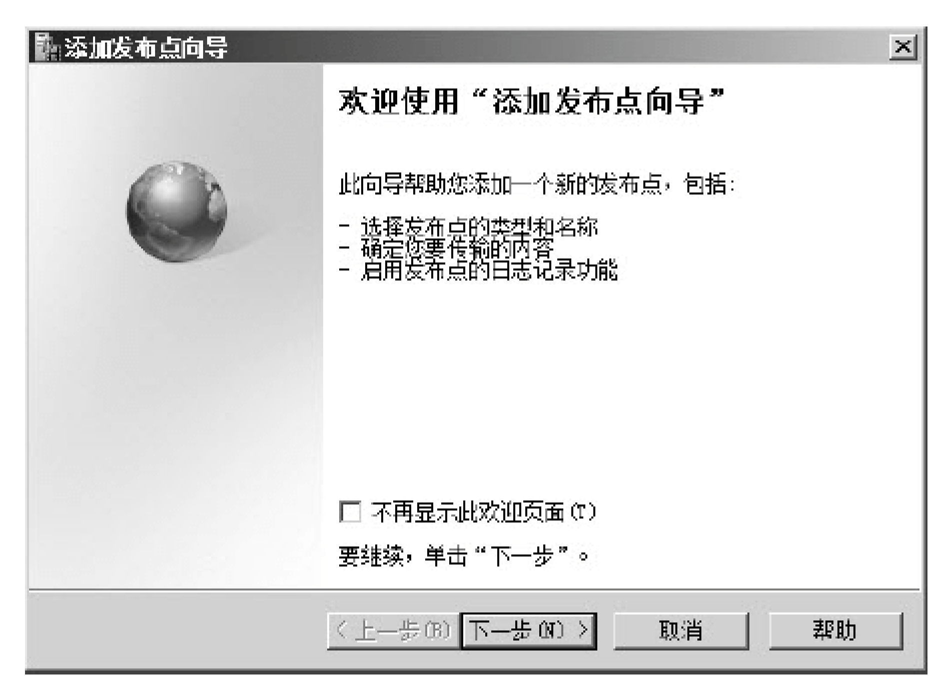


图 11-11　“添加发布点向导”对话框的欢迎界面

(3) 单击“下一步”按钮，进入“发布点名称”设置界面，输入发布点名称，如图 11-12 所示。

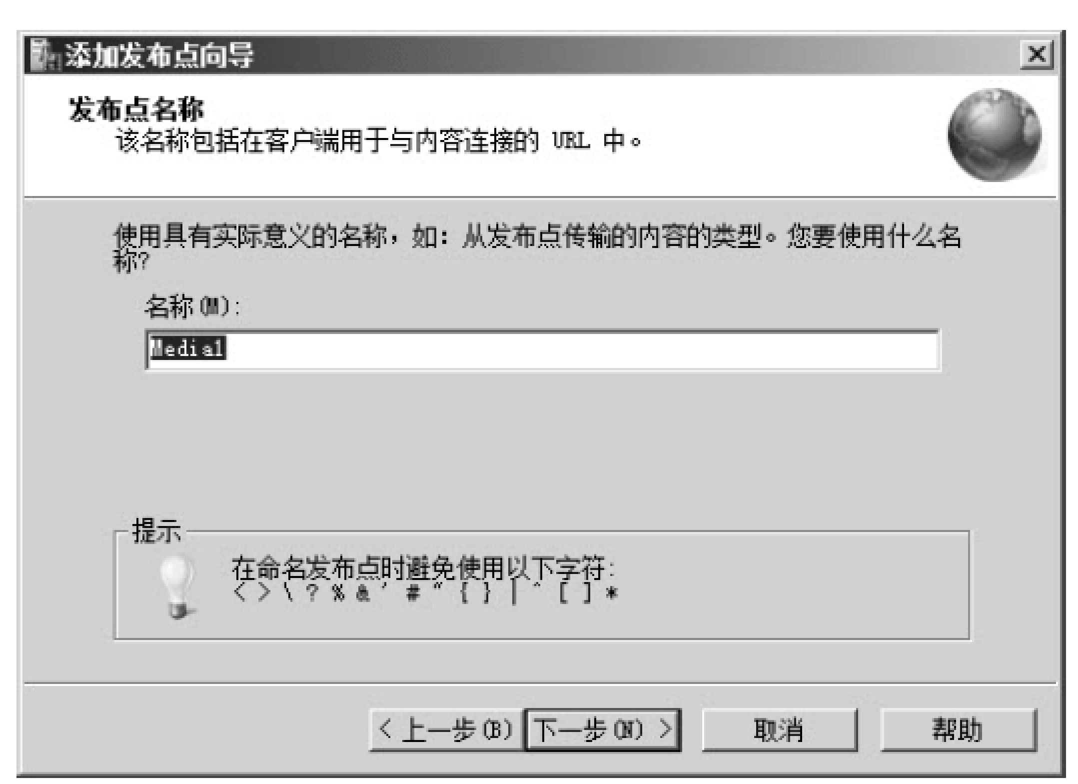


图 11-12　“发布点名称”界面

(4) 单击“下一步”按钮，进入“内容类型”界面，选择发布内容的类型，如图 11-13 所示。

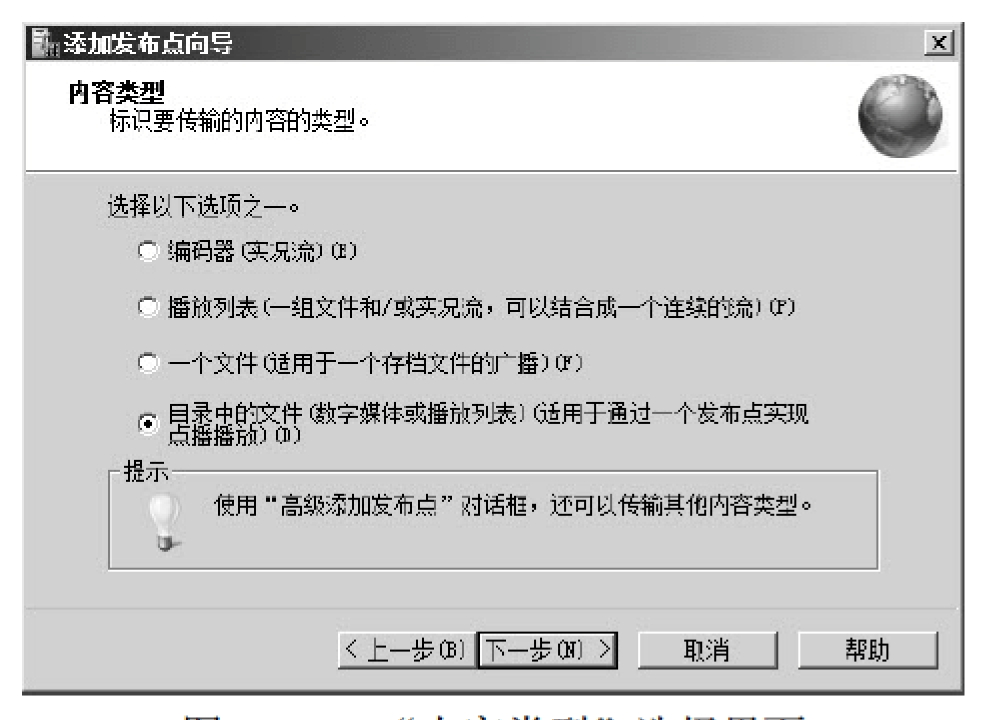


图 11-13　“内容类型”选择界面

本窗口一共有以下 4 个选项。

- 编码器：允许服务器连接到一台编码计算机，并发布由该计算机编码的音视频文件；
- 播放列表：将一组音频和视频文件的存储位置信息集合起来，生成一个播放列表，站点可以调用该播放列表，从而播放多个文件；
- 一个文件：站点只发布一个音视频文件；
- 目录中的文件：发布一个目录中的所有音视频文件及播放列表所指向的多媒体文件。

(5) 选中“目录中的文件”单选按钮，然后单击“下一步”按钮，进入“发布点类型”界面，如图 11-14 所示；

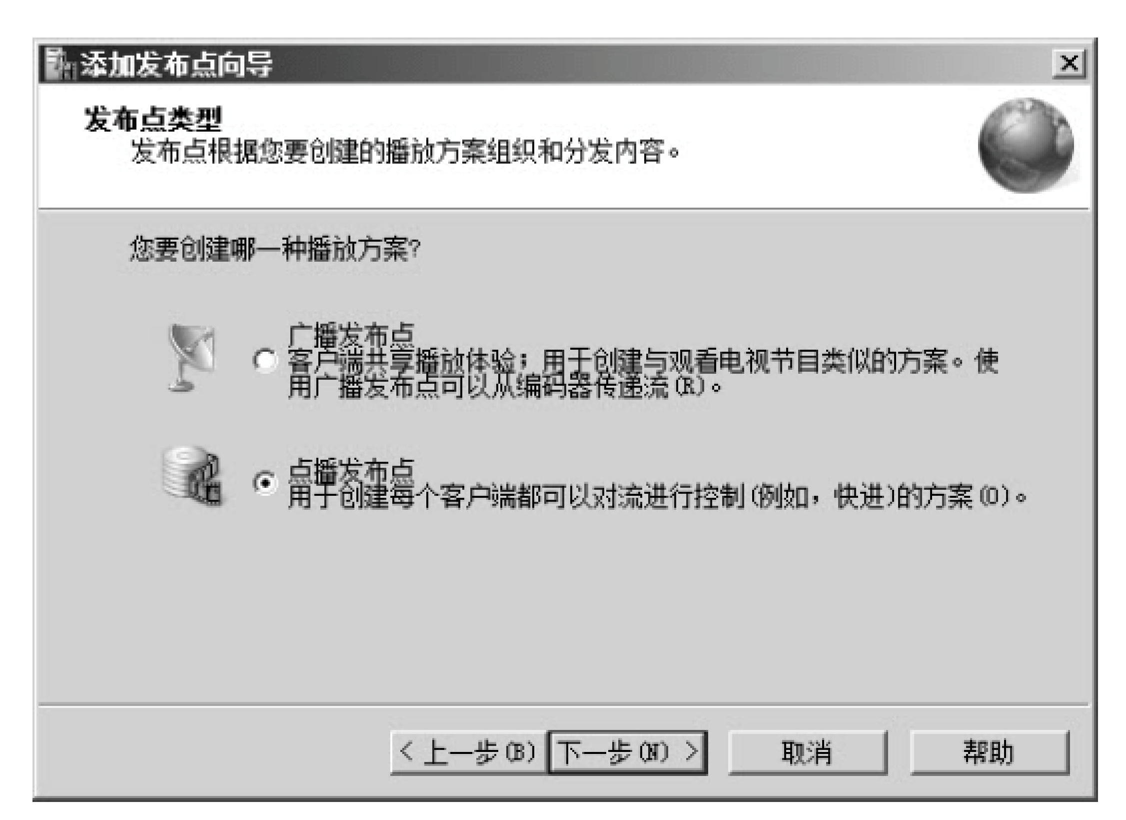


图 11-14　“发布点类型”界面

(6) 选中“点播发布点”单选按钮，单击“下一步”按钮，进入“目录位置”界面，如图 11-15 所示。

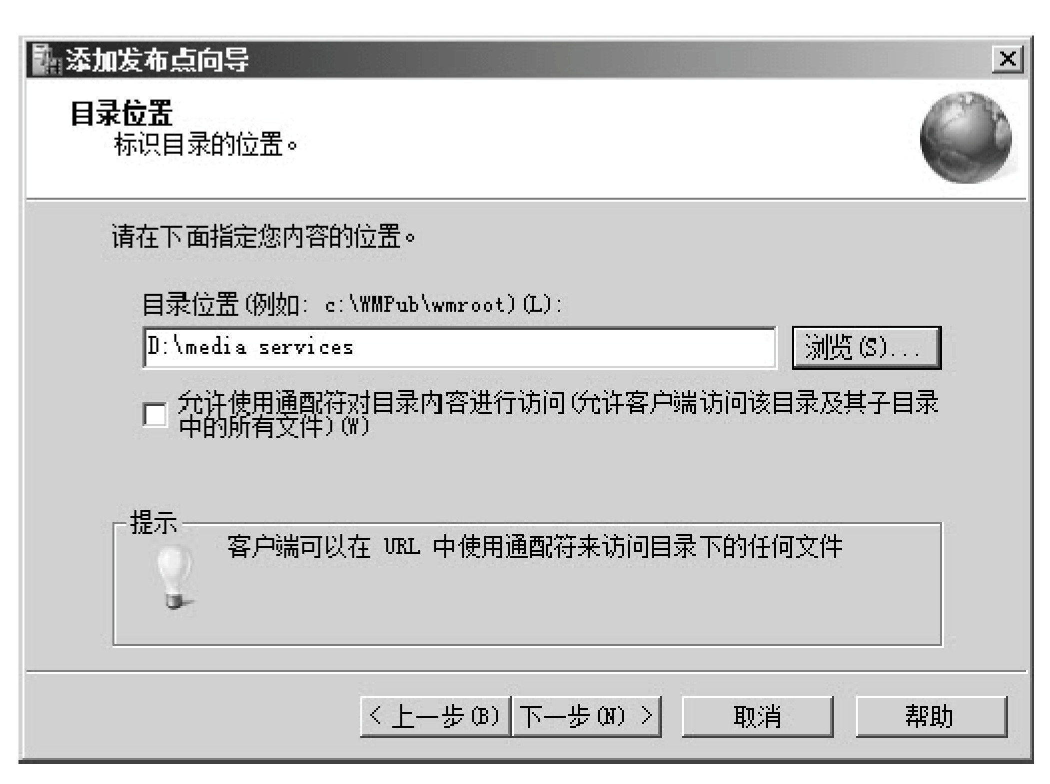


图 11-15　“目录位置”界面

(7) 设置好放置要发布的音视频文件所在的路径后，单击“下一步”按钮，进入“内容播放”界面，如图 11-16 所示。

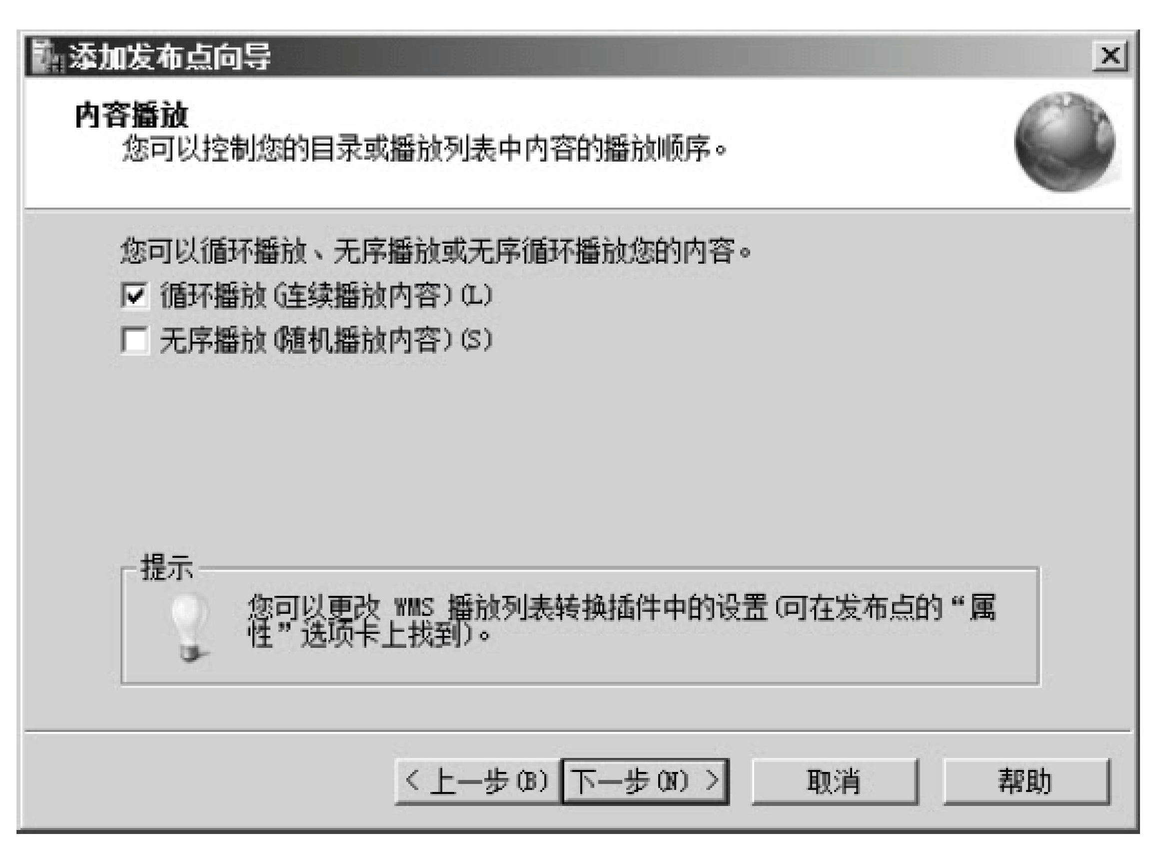


图 11-16　“内容播放”界面

(8) 选中“循环播放(连续播放内容)”复选框，如果想随机播放文件，可以选中“无序播放(连续播放内容)”复选框，单击“下一步”按钮，进入“单播日志记录”界面，如图 11-17 所示。

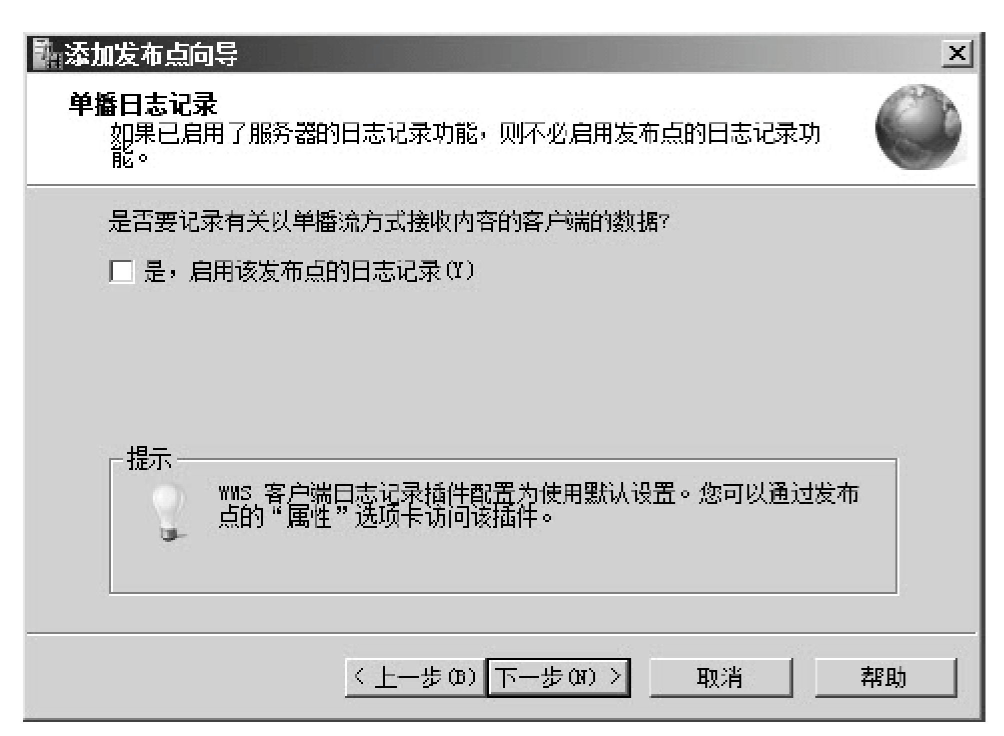


图 11-17　“单播日志记录”界面

(9) 不做选择，则服务器不会记录客户端的相关数据，单击“下一步”按钮，进入“发布点摘要”界面，如图 11-18 所示。

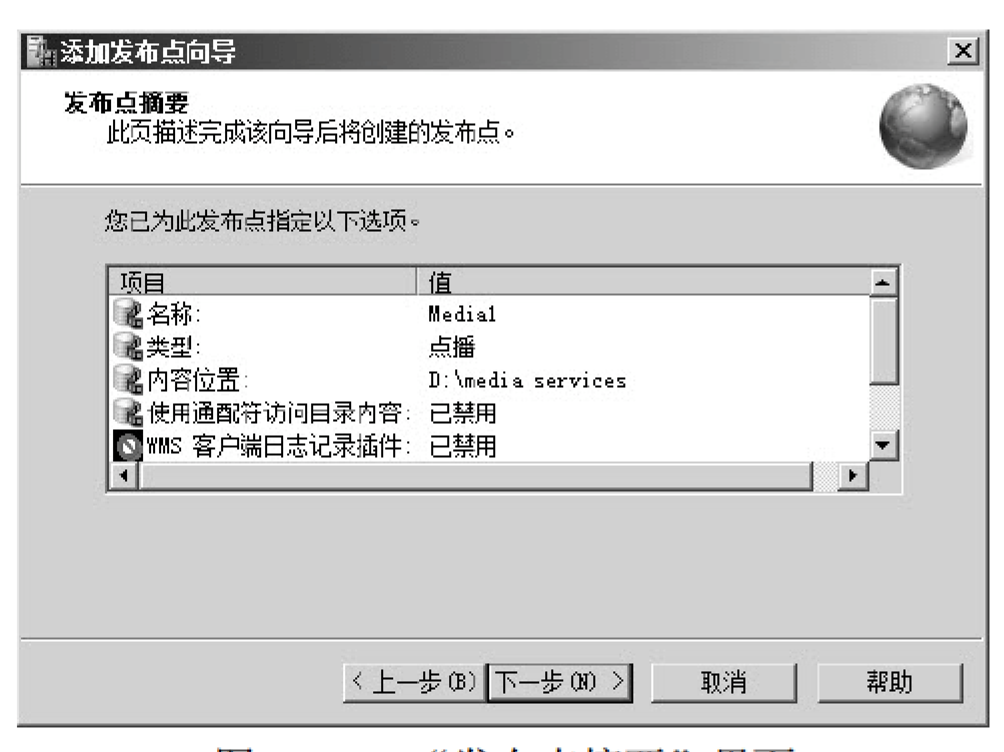


图 11-18　“发布点摘要”界面

(10) 如果有需要修改的部分，单击“上一步”按钮返回并修改，如果没有需要修改的部分，单击“下一步”按钮，进入完成界面，如图 11-19 所示。

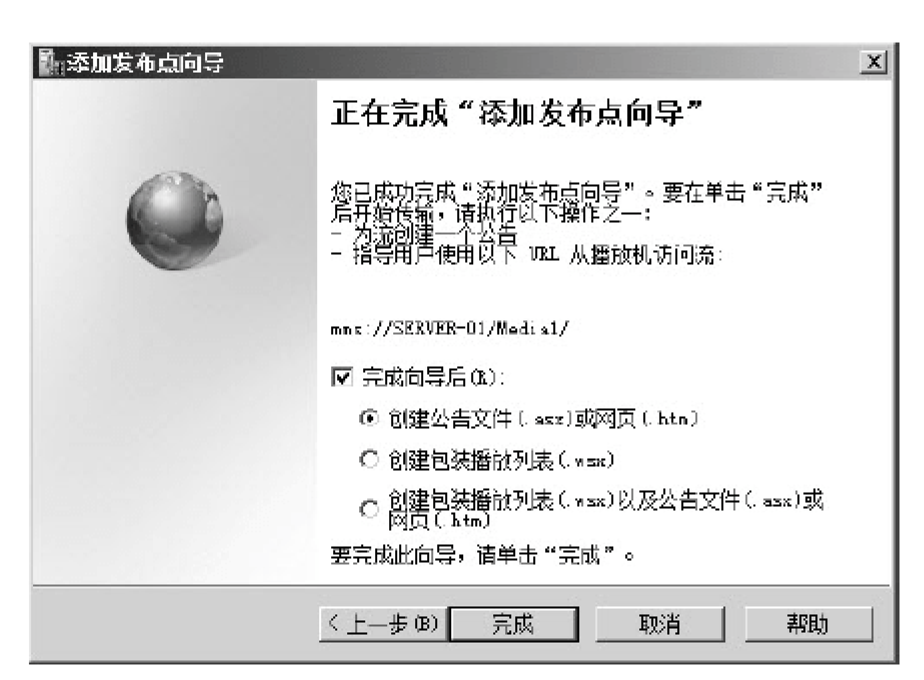


图 11-19　向导完成界面

(11) 选中“完成向导后”和“创建公告文件或网页”，单击“完成”按钮，进入“单播公告向导”界面，如图 11-20 所示。



图 11-20　“单播公告向导”欢迎界面

(12) 单击“下一步”按钮，进入“点播目录”界面，如图 11-21 所示。



图 11-21　“点播目录”界面

(13) 选择要公告的文件，如果要公告所有文件，则需要在第(6)步中允许使用通配符访问站点文件，或先配置站点属性后再发布公告。单击“下一步”按钮，进入“访问该内容”

界面，如图 11-22 所示。

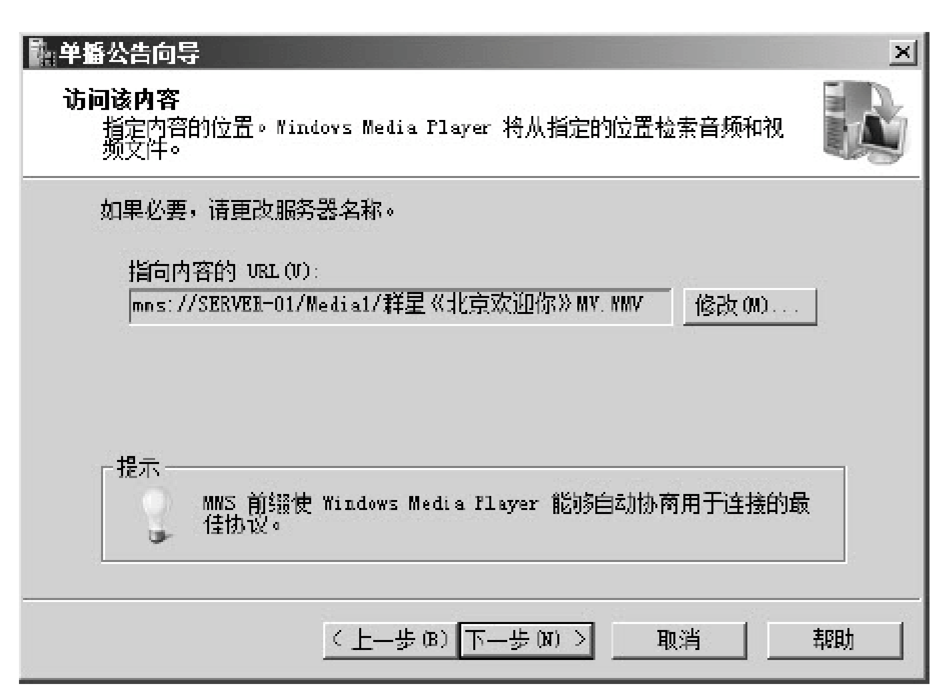


图 11-22　“访问该内容”界面

(14) 该窗口指定了用户可以在网络上访问发布的文件的 URL，如需更改则单击“修改”按钮，更改 URL，如不需要更改则单击“下一步”按钮，进入“保存公告选项”界面，如图 11-23 所示。

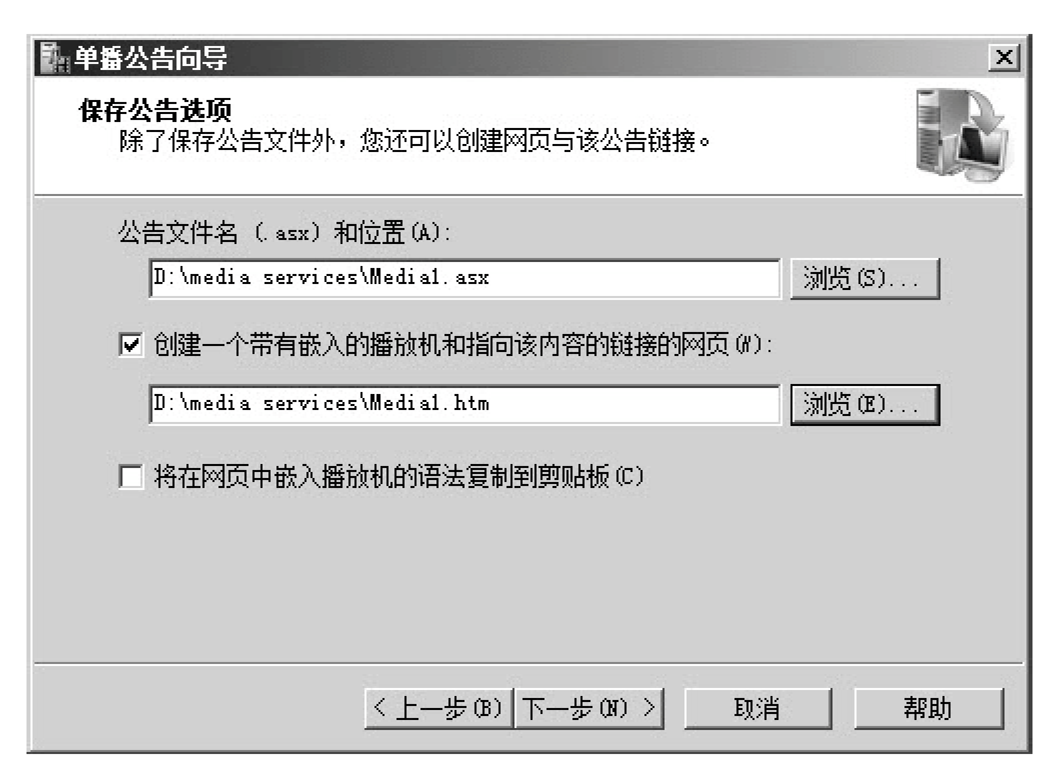


图 11-23　“保存公告选项”界面

(15) 设置保存的公告文件名和存储位置后，同时选中“创建一个带有嵌入的播放机和指向该内容的链接的网页”，设置保存的文件名称及路径，单击“下一步”按钮，进入“编辑公告元数据”界面，如图 11-24 所示。



图 11-24　“编辑公告元数据”界面

(16) 设置元数据内容，单击“下一步”按钮，进入完成界面，如图 11-25 所示。



图 11-25　向导完成界面

(17) 选中“完成此向导后测试文件”复选框，单击“完成”按钮，完成配置并开始测试，如图 11-26 所示。单击“测试”按钮，可测试相应的项目。

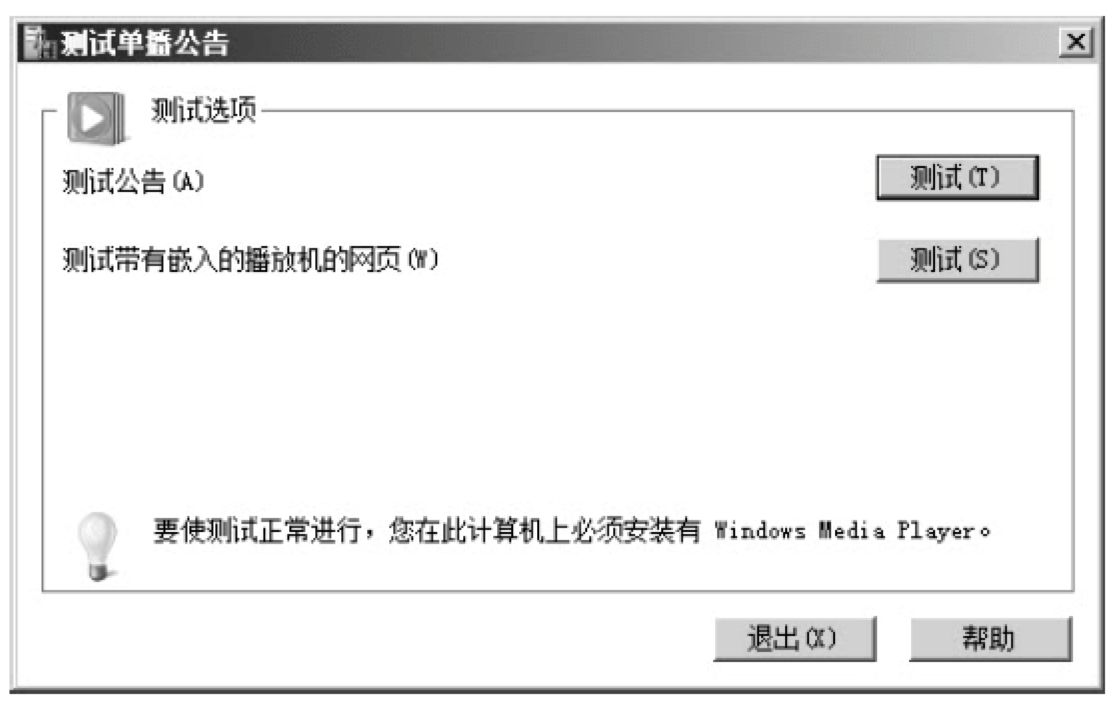


图 11-26　“测试单播公告”界面

(18) 进行“测试公告”时，会打开媒体播放器 Windows Media Player 或兼容的播放器，所以如果没有安装播放器将无法测试；进行“测试带有嵌入的播放机的网页”时，最好使用 Microsoft 公司的 IE 浏览器，而且使用 IE 浏览器时可能会弹出信息，提示用户 IE 已经自动限制了一些脚本和控件的运行，需设置浏览器允许运行这些被阻止的内容。测试通过，则说明流媒体站点创建成功，可以使用。

11.2.2　实现视频和音频广播

如果采用向导设置广播站点，基本流程和创建点播站点相似，仅仅在设置“发布点类型”时选择“广播发布点”以及设置传递数据的方式为单播或多播，其他部分没有区别，这里不再赘述。下面学习一种新的创建方式。

(1) 打开“Windows Media 服务”窗口，右击“发布点”，在弹出的快捷菜单中选择“添加发布点(高级)”命令，打开“添加发布点”对话框，如图 11-27 所示。



图 11-27　“添加发布点”对话框

(2) 将“发布类型”设置为“广播”，设置发布点名称为 Media2，选择合适的内容类型以及内容位置。单击“确定”按钮，完成基本配置。此时“Windows Media 服务”对话框中已经显示新建站点的相关信息了，如图 11-28 所示。



图 11-28　“发布站点”管理界面

(3) “监视”选项卡显示了当前站点的运行状态，最下方的按钮可以控制当前站点，依次是“启动发布点”按钮、“停止发布点”按钮、“允许新的单播连接”按钮、“拒绝新的单播连接”按钮、“断开所有客户端连接”按钮、“重置所有计数器”按钮、“查看性能监视器”按钮和“帮助”按钮。

(4) 打开“源”选项卡，单击其中的“更改”按钮，即可更改发布内容，但更改前必须关闭当前站点，如图 11-29 所示。



图 11-29　“源”选项卡

(5) “公告”选项卡用于设置单播流和多播流的公告，如图 11-30 所示，可以通过相应的向导来创建公告。



图 11-30　“公告”选项卡

(6) 打开“属性”选项卡，如图 11-31 所示。

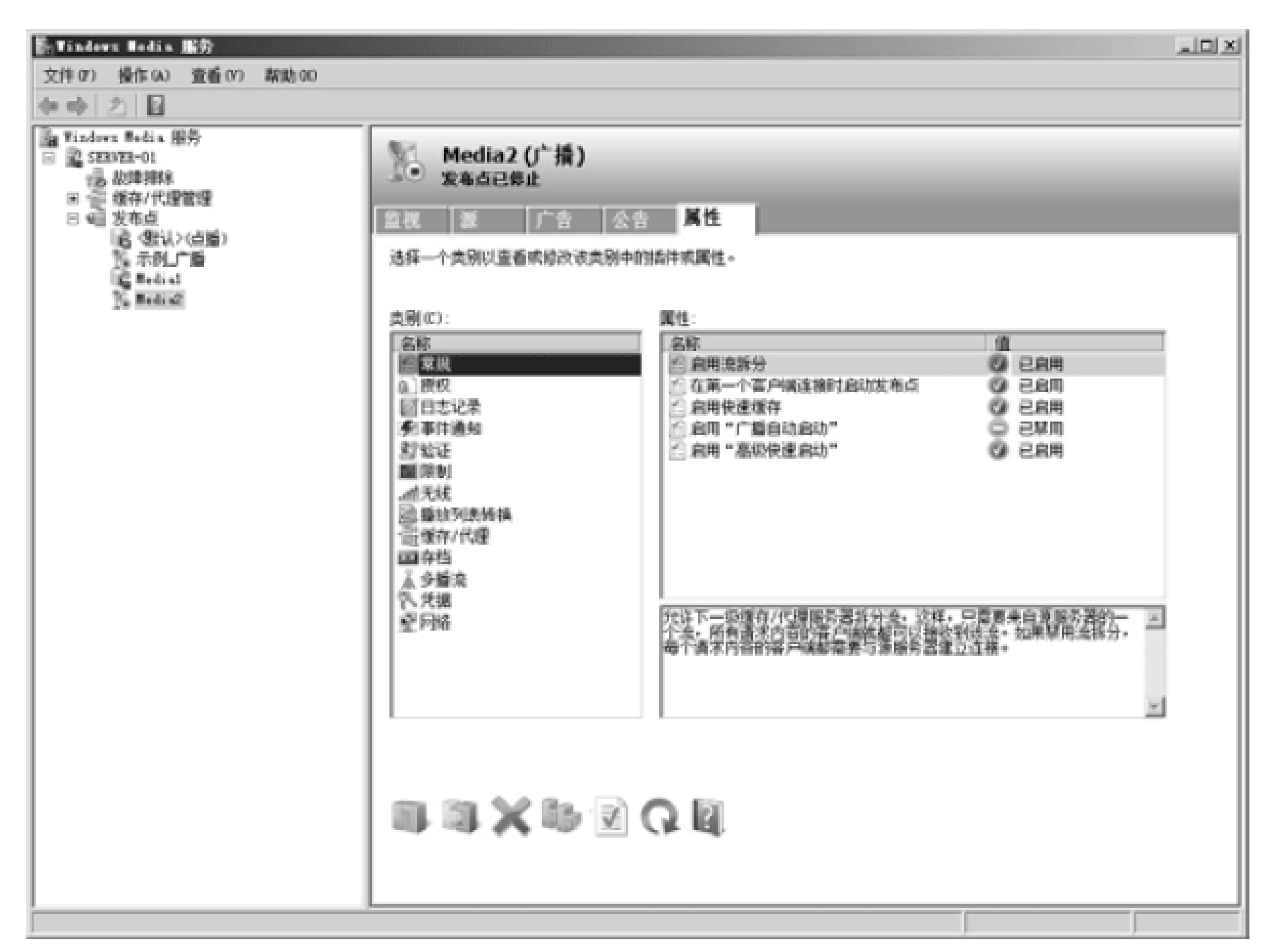


图 11-31　“属性”选项卡

(7) 在“属性”选项卡中可以设置更多内容，一般来说，如果没有特殊情况，保持默认设置即可。

11.2.3　制作播放列表

简单来说，播放列表就是一个文件，其中存储了某个媒体文件的存储位置。当服务器或者播放器打开播放列表时就会根据其中的记录找到相应的媒体文件并播放。这种模式下，只要有一个播放列表，就可以将多个媒体文件组织在一起，即使它们不在同一目录下，也可以很方便的调用。制作播放列表的步骤如下：

(1) 打开“Windows Media 服务”窗口，选择“发布点”节点，在右侧窗口中选择“察看播放列表编辑器”，即如图 11-32 所示中方框标出的按钮。



图 11-32　“发布点”管理界面

(2) 单击该按钮后，打开 Windows Media 播放列表编辑器，如图 11-33 所示。

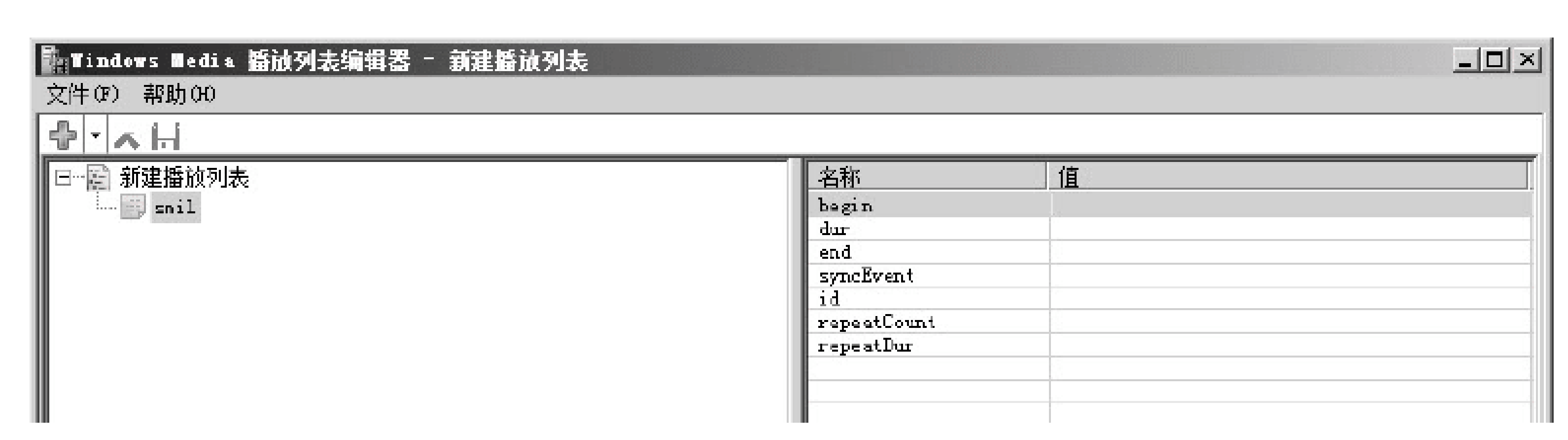


图 11-33　“播放列表编辑器”界面

(3) Windows Media 播放列表是使用XML语言描述的，在编辑器中罗列了常用的XML元素，这些元素如下。

- smil：smil 是同步多媒体集成语言的建成，表示播放列表的根元素；
- begin：制定 smil 元素何时启用，用时间值表示，单位是秒；
- dur：指定元素的持续时间；
- end：制定 smil 元素何时禁用，即变为未激活元素；
- syncEvent：制定一个字符串，用于触发包装播放列表中某个元素的开始或结束；
- id：为 smil 元素指定一个名称，供其他元素或播放列表引用；
- repeatCount：指定播放列表在停止前重复播放的次数；
- repeatDur：指定播放列表在停止之前重复播放的时间长度。

如果对这些元素的作用不清楚，可以不作设置，或者使用向导创建流媒体站点，不需要对这些元素加以修改。

(4) 在“smil”上右击，在弹出的快捷菜单中选择“添加媒体”命令，打开“添加媒体元素”对话框，如图 11-34 所示。



图 11-34　“添加媒体元素”对话框

(5) 在对话框中指定媒体元素的类型和媒体文件的路径，单击“确定”按钮，返回播放列表编辑器，如图 11-35 所示。



图 11-35　“播放列表编辑器”界面

(6) 依次选择“文件”→“保存”命令，打开“另存为”对话框，如图 11-36 所示。



图 11-36　“另存为”对话框

(7) 设置播放列表的文件名和存储路径后，单击“保存”按钮，关闭 Windows Media 播放列表编辑器，完成播放列表的创建。

11.2.4　发布广告

报纸、无线电广播和电视行业都能够产生收益并以低成本为公众提供信息服务，因为它们能够找到支付费用以发布产品广告的赞助商。因特网也包含了这种商务模式，大多数网站也都包含有某种形式的广告。提供信息服务的网站通过广告销售为其运作提供资金，一些公司和电子商务站点也可通过广告为自己的品牌进行市场宣传。

Windows Media Services 通过以下几种方式为广告提供支持。

- 播放列表：也称为间隙广告，播放列表为在广播期间播放插播式广告提供了一种简易方法。动态播放列表可以响应客户端的用户配置文件，以便根据人数统计信息有目的地发布广告。
- 包装：包装可用来在客户端请求的内容开始和结束时提供一组广告。包装通常用来实现跟片广告或引入/引出广告。
- 报告：详细的日志文件和实时性能计数器提供了一种监视网站活动与评估观众的方法。反映点击次数、播放次数和客户端收看广告的时间长度的计数器可供用户在计费与生成报告时使用。

在设置广告之前，先准备好作为广告素材的视频文件或者图片文件，本例中准备 3 张 jpg 图片作为广告素材。

如果想在用户点播影片的过程中插播广告，可以在播放列表中添加广告，步骤如下：

(1) 打开“Windows Media 服务”对话框，定位到一个“发布点”，单击打开“源”选项卡，如图 11-37 所示。



图 11-37　“源”选项卡

(2) 单击下方的“查看播放列表编辑器”按钮，打开“播放列表”对话框，如图 11-38 所示，选中“打开现有播放列表”单选按钮，浏览选择前面保存的播放列表文件。



图 11-38　“播放列表”对话框

(3) 单击“确定”按钮，打开“Windows Media 播放列表编辑器”，如图 11-39 所示。

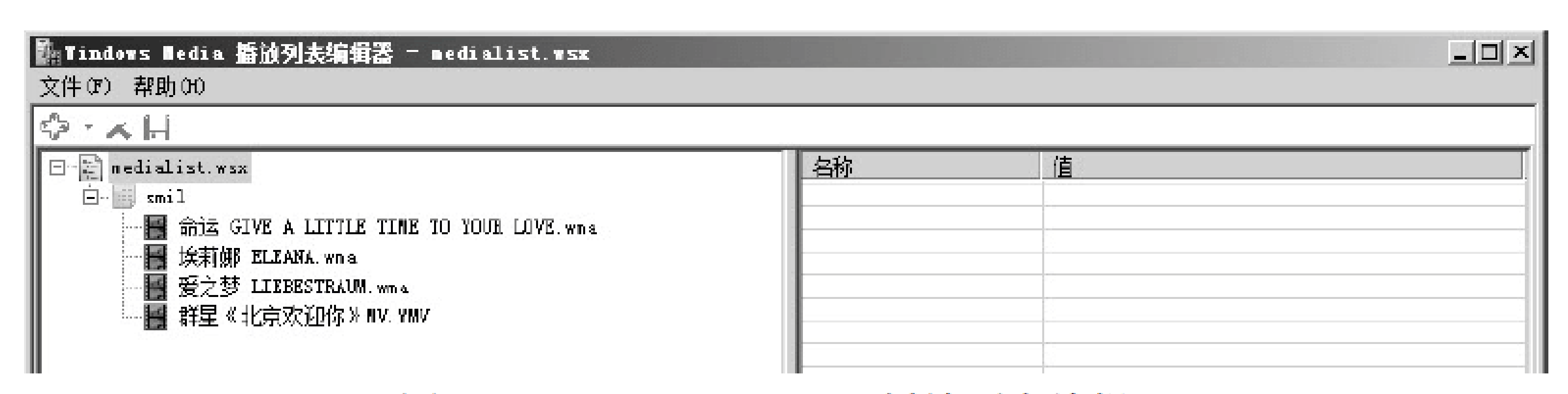


图 11-39　Windows Media 播放列表编辑器

(4) 右击“smil”节点，在弹出的快捷菜单中选择“添加广告”命令，打开“添加广告”对话框，在文本框中输入要添加的广告文件的路径，如图 11-40 所示。



图 11-40　“添加广告”对话框

(5) 单击“确定”按钮，返回“Windows Media 播放列表编辑器”，然后将添加的广告移至列表头部，如图 11-41 所示。

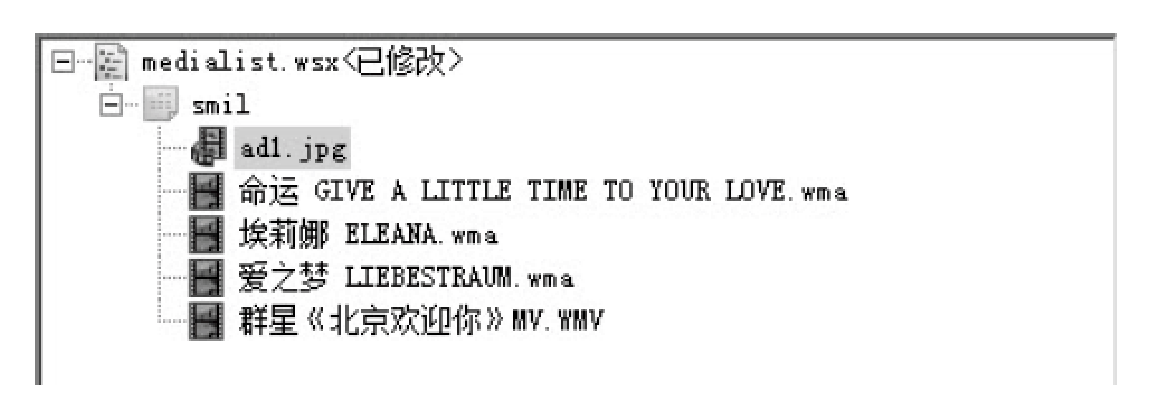


图 11-41　媒体播放顺序播放界面

(6) 至此，添加广告的基本设置已经完成。还可以通过在右侧窗口中调整广告文件的属性，以实现更高级的功能，如将广告文件的“no Skip”属性值设置为“TRUE”，则播放到此媒体时，不允许跳过。当终端用户播放到此元素时，播放器软件上的“前进”、“后退”、“下一个”等控制按键将不起作用。

(7) 重复以上步骤，可以添加多个广告并调整其播放次序。设置完毕后，保存并退出即可。将来使用该播放列表的流媒体站点就可以播放广告了。

还可以在 Windows Media Services 2008 中使用包装广告，当用户首次连接到服务器或内容流结束时，可以使用包装来提供广告或其他内容。在为内容指定一个包装时，Windows Media Services 2008 将把该内容作为包装播放列表的一部分包含在其中。通过使用包装播放列表，可以将所选的序幕内容和结尾内容作为播放列表项目插入到主内容前后。

除广告外，常作为包装播放的内容还有由 Active Server Page(ASP)生成的动态播放列表、站点商标以及赞助商标识。例如，假设单播客户端连接到已指定了包装广告的实况流，那么它只有在播放完包装播放列表中指定的所有内容后才能播放实况内容。

使用包装广告的具体操作步骤如下：

(1) 在“Windows Media 服务”窗口中，定位到一个发布点，打开“广告”选项卡，如图 11-42 所示。



图 11-42　“广告”选项卡

(2) 单击下方的“包装编辑器”按钮，打开“包装播放列表编辑器选项”对话框，取消“使用‘创建包装向导’”复选框，如图 11-43 所示。



图 11-43　“包装播放列表编辑器选项”对话框

(3) 单击“确定”按钮，打开“Windows Media 播放列表编辑器”，如图 11-44 所示。



图 11-44　“Windows Media 播放列表编辑器”界面

(4) 在“smil”节点上右击，在弹出的快捷菜单中选择“添加广告”命令，打开“添加广告”对话框，在其中的文本框中输入广告文件的路径，如图 11-45 所示。



图 11-45　“添加广告”对话框

(5) 单击“确定”按钮，返回播放列表编辑器，将广告在列表中移动到最前面，然后保存播放列表至广告文件所在文件夹，返回发布点的“广告”选项卡，单击“更改”按钮，引用刚创建好的播放列表，如图 11-46 所示。

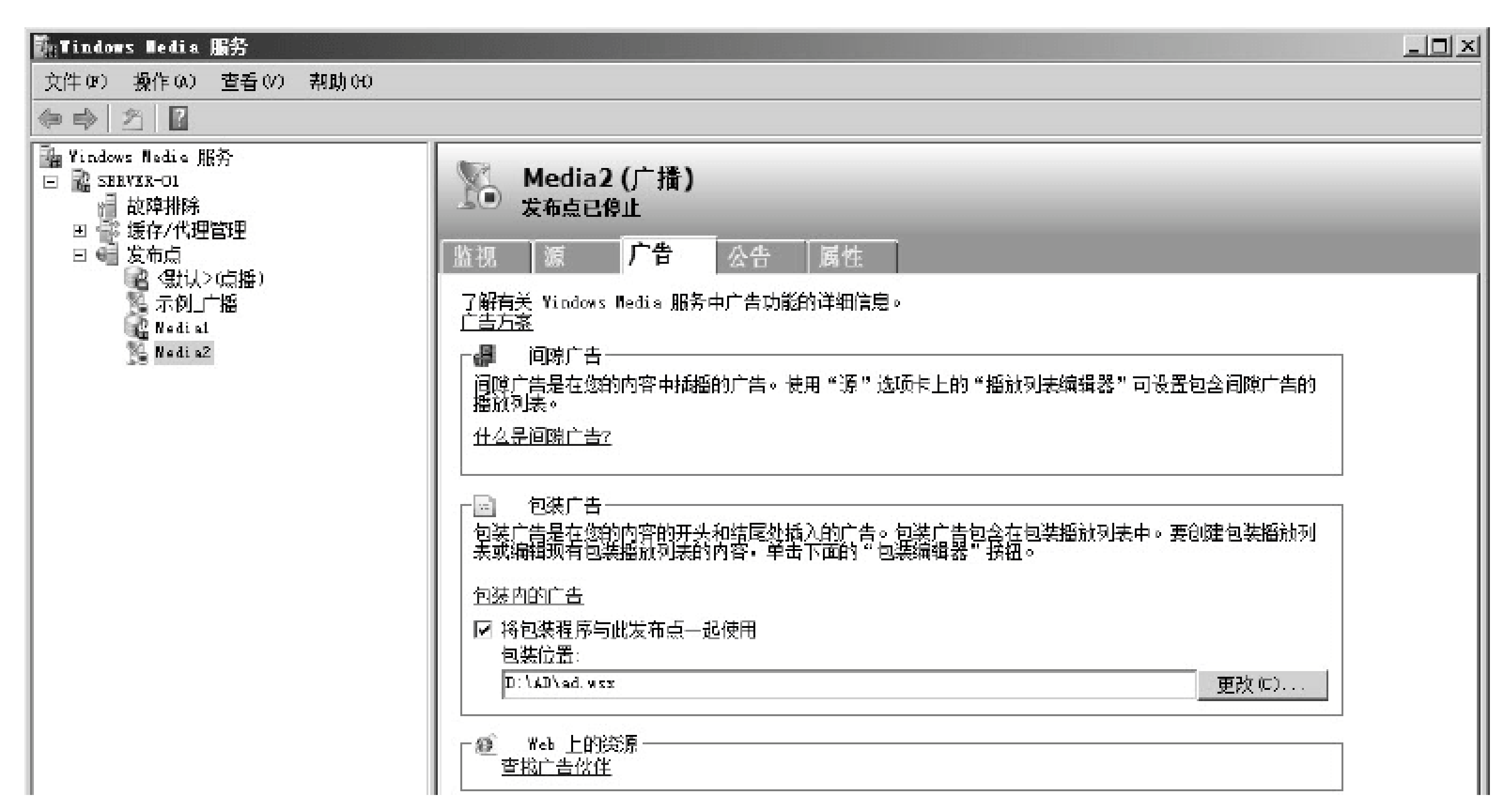


图 11-46　“广告”选项卡

(6) 至此，包装广告添加完毕。

如果启用“属性”选项卡中的“日志记录”功能，就可通过日志跟踪广告发布的效果了。

11.2.5　对点播发布点的访问

打开发布点的“公告”选项卡，如图 11-47 所示。

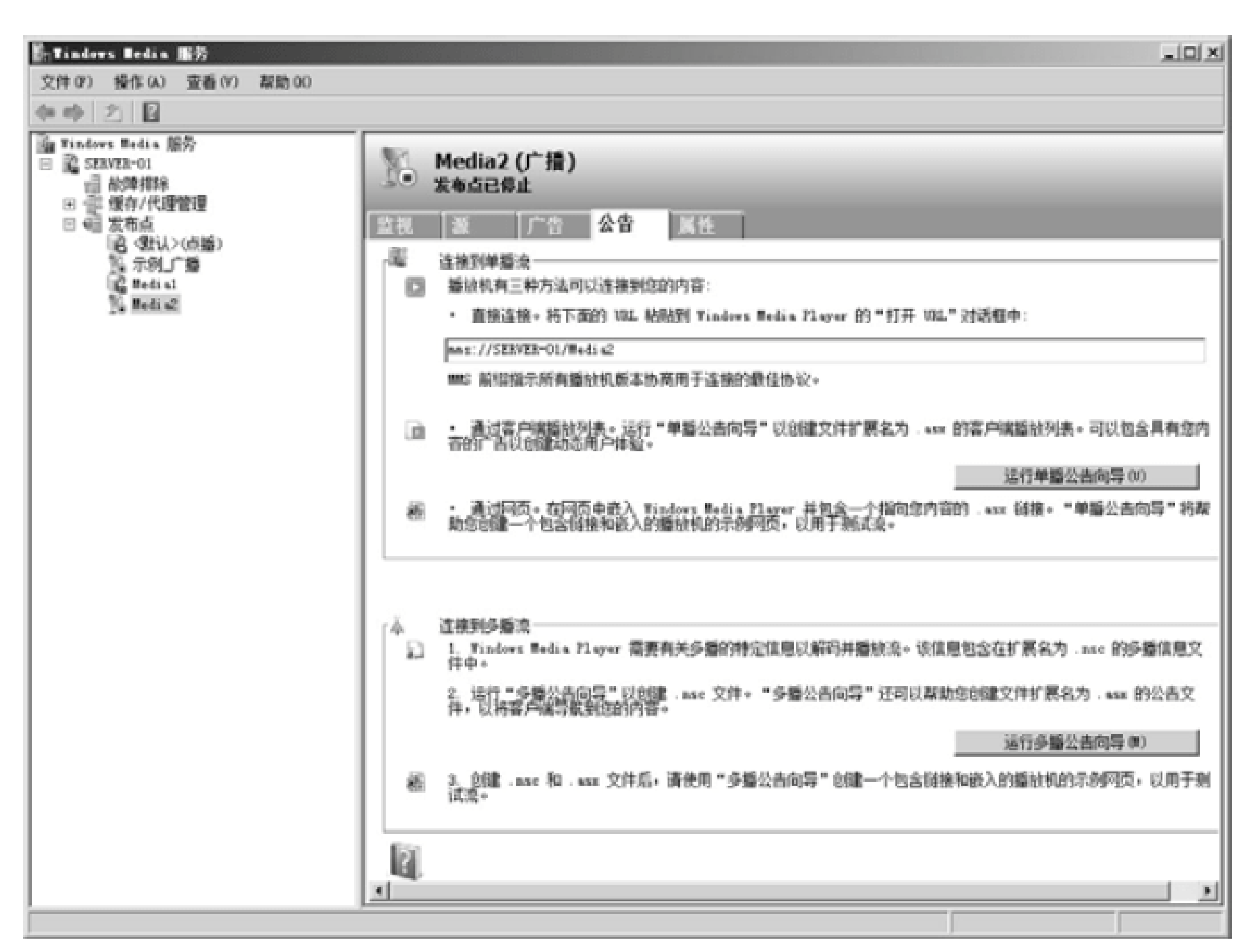


图 11-47　“公告”选项卡

单击“运行单播公告向导”和“运行多播公告向导”按钮，可以使用向导分别创建公告和包含视频插件网页，创建完毕后，可以使用“公告”选项卡中提示的地址(mms 开头的地址)使用播放器直接访问站点，也可以利用向导生成的网页，将视频在网页上播放。

11.3　本章小结

本章介绍了在 Windows Server 2008 服务器上安装和使用流媒体服务的基本方法。Windows Media 流媒体技术不仅可以实现视频和音频的网络播放，还可以由管理员控制播放模式，添加广告等。用户则可以利用播放器或网页来访问这些流媒体信息。

(1) 流媒体服务的安装：本节介绍了 Windows Server 2008 下安装流媒体服务的基本方法，通过学习，学生可以掌握从微软网站下载流媒体服务组件并进行安装的基本步骤，能够正确区分点播和广播，并能够根据网络环境选择合适的模式。

(2) 实现点播和广播：本节介绍了流媒体服务器的设置方法，通过学习，学生可以掌握实现各种播放方式的基本方法，并可以在视频中设置广告，以及访问流媒体的方法。

11.4　思考与练习

【思考题】

1. 常见流媒体技术和流媒体传输协议有哪些？
2. 点播和广播的区别是什么？
3. Windows Media Services 2008 具有哪些功能？

【练习题】

1. 如何在 Windows Server 2008 上安装流媒体服务器组件？
2. 如何在流媒体中播放广告？
3. 怎样制作播放列表？
4. 如何访问流媒体服务器上的视频或音频？

第12章　终端服务

【本章导读】

在局域网规模相对较大的工作环境中，如果客户端工作站安装了不同的操作系统，分别在这些系统环境中安装部署相同版本的应用程序时，工作量无疑是十分巨大的。为了有效提高网络管理效率，可以利用终端服务来解决应用程序集中部署的难题，终端服务是在Windows NT 中首先引入的一个服务。终端服务使用 RDP 协议(远程桌面协议)客户端连接，使用终端服务的客户可以在远程以图形界面的方式访问服务器，并且可以调用服务器中的应用程序、组件、服务等，和操作本机系统一样。这样的访问方式不仅大大方便了各类用户，还有效地节约了成本。

12.1　部署终端服务器

12.1.1　终端服务概述

局域网工作站需要使用的应用程序只要集中在终端服务器中安装、部署一次，无论工作站使用了什么类型的操作系统，都能通过远程终端访问实现使用应用程序的目的。伴随着Windows Server 2008 系统的面世，系统终端服务功能也明显得到了强化。

借助终端服务，网络管理员根本不需要在局域网中的每一台工作站中安装和维护同样的应用程序，如果客户端用户需要集中使用某一个应用程序，网络管理员只要将该应用程序集中在终端服务器中安装部署一次就可以了，客户端用户到时只要通过终端服务就能在本地系统运行应用程序了；借助终端服务，客户端用户能够非常方便地使用终端服务器中的各种共享资源，而不需要额外增加使用成本，从而有效地节约了办公成本；借助终端服务，单位不需要耗费大量的财力、物力在局域网中的所有客户端工作站中安装部署单位的业务程序，而只需要一次性地在终端服务器中安装部署就可以了，这样就能够简化局域网管理维护工作量，减少网络维护成本以及降低复杂程度。终端服务的目的是为了实现集中化应用程序的访问。终端服务主要应用于以下几种环境中。

(1) 应用程序集中部署：在客户端/服务器网络体系中，如果客户端需要使用相同的应用程序，比如要使用相同版本的邮件客户端、办公软件等，而客户端部署的操作系统又不尽相同，如 Windows 2000、Windows XP、Windows Vista等，这时候如果网络规模很大，分别向这些客户端部署相同版本的应用软件是件让管理员非常头痛的事情，需要大量重复的工作，而且需要考虑软件版本的兼容性问题。这时候如果采用终端服务则可以很好地解

决这个问题，客户端需要使用的应用软件只需在终端服务器上部署一次，无论客户端安装什么版本的操作系统，都可以连接到终端服务器使用特定版本的应用软件。

(2) 分支机构方便利用：企业分支机构一般没有或者只有很少的专业 IT 管理员，企业如果向各个分支机构委派专门的网络管理员，无疑会使企业增加不小的开支。这时候如果分支机构的计算机均采用终端服务的解决方案，统一连接到终端服务器应用特定软件，可以简化 IT 管理维护，减少维护成本和复杂程度。

(3) 任意地点的安全访问：很多时候出差在外的员工需要应用某个特性的应用软件，如公司定制的财务软件等，这时候员工可以通过手机、笔记本电脑等移动设备，在任意地点连接公司终端服务器进行应用。如在 Windows Server 2008 中，用户可以利用终端服务中的 TS Web Access 功能，没必要连接 VPN，仅仅通过 Web 方式即可访问企业终端服务器，并且可以获得良好的用户体验。此外，Windows Server 2008 中的终端服务具有网关功能 TS Gateway，可以裁决用户是否满足连接条件，并且可以确定用户可以连接哪些终端服务器，保证了安全性。

与传统的终端服务功能相比，Windows Server 2008 系统在这方面的功能明显得到了增强。例如，在 Windows Server 2008 系统环境下，客户端用户能够使用内置在终端服务中的 Ts Web Access 功能，来实现通过 Web 方式访问单位局域网终端服务器的目的，突破了以往只能通过远程桌面连接访问终端服务器的限制，通过这种访问方式，客户端用户能够享受到良好的用户体验。此外，Windows Server 2008 系统的终端服务还新增加了 TS Gateway 网关功能，该功能能够判断出客户端用户是否满足网络连接条件，并且能够确定用户究竟能够访问哪些终端服务器，从而有效保证了终端访问的安全性。

12.1.2　部署终端服务器

在 Windows 2000、Windows 2003 中部署终端服务，其客户端不需要进行太多的设置，只需要客户端具有远程桌面功能即可，远程桌面功能在 Windows 2000 Pro、Windows XP Pro 中均已经集成，Windows 98 客户端则需要单独进行安装。在 Windows 2008 中，终端服务有了比较大的改进，用户可以通过 Web、远程桌面、终端服务器所创建的 rdp 或者 msi 文件进行连接。如果用户需要通过远程桌面进行连接，客户端需要安装远程桌面 6.0 以上版本。在 Vista 和 Windows 2008 以及 Windows XP SP3 中均已经整合远程桌面 6.0，Windows XP SP2 客户端用户可以通过微软网站下载安装。

远程桌面 6.0 在功能性上相对以前的版本进行了加强，如增强了服务器身份验证、设置终端服务网关、即插即用设备的重定向功能，并且配合 Windows 2008 终端服务可以获得类似 Vista 的用户体验。运行 mstsc 命令可以打开远程桌面 6.0 控制台。

用户可以使用远程桌面连接或 TS RemoteApp，从公司网络内部或 Internet 访问终端服务器，连接到终端服务器来运行程序、保存文件以及使用该服务器上的网络资源。

通过 TS Web Access，用户可以通过访问网站(从 Internet 或 Intranet)访问可用 RemoteApp 程序的列表。若要启动 RemoteApp 程序，只需单击相应的程序图标。在启动 RemoteApp

程序时，将在托管 RemoteApp 程序的终端服务器上启动终端服务会话。

安装终端服务的步骤如下：

(1) 以超级管理员权限如 administrator 帐户登录 Windows Server 2008 系统，单击“开始”按钮，选择“程序”→“管理工具”→“服务器管理器”，进入“服务器管理器”控制台窗口，如图 12-1 所示，可以集中管理 Windows Server 2008 服务器系统中的各个角色以及各项功能。



图 12-1　“服务器管理器”控制台窗口

(2) 单击窗口左侧列表区域中的“角色”节点，在右侧列表中，单击“添加角色”按钮，“进入添加角色向导”对话框，如图 12-2 所示。

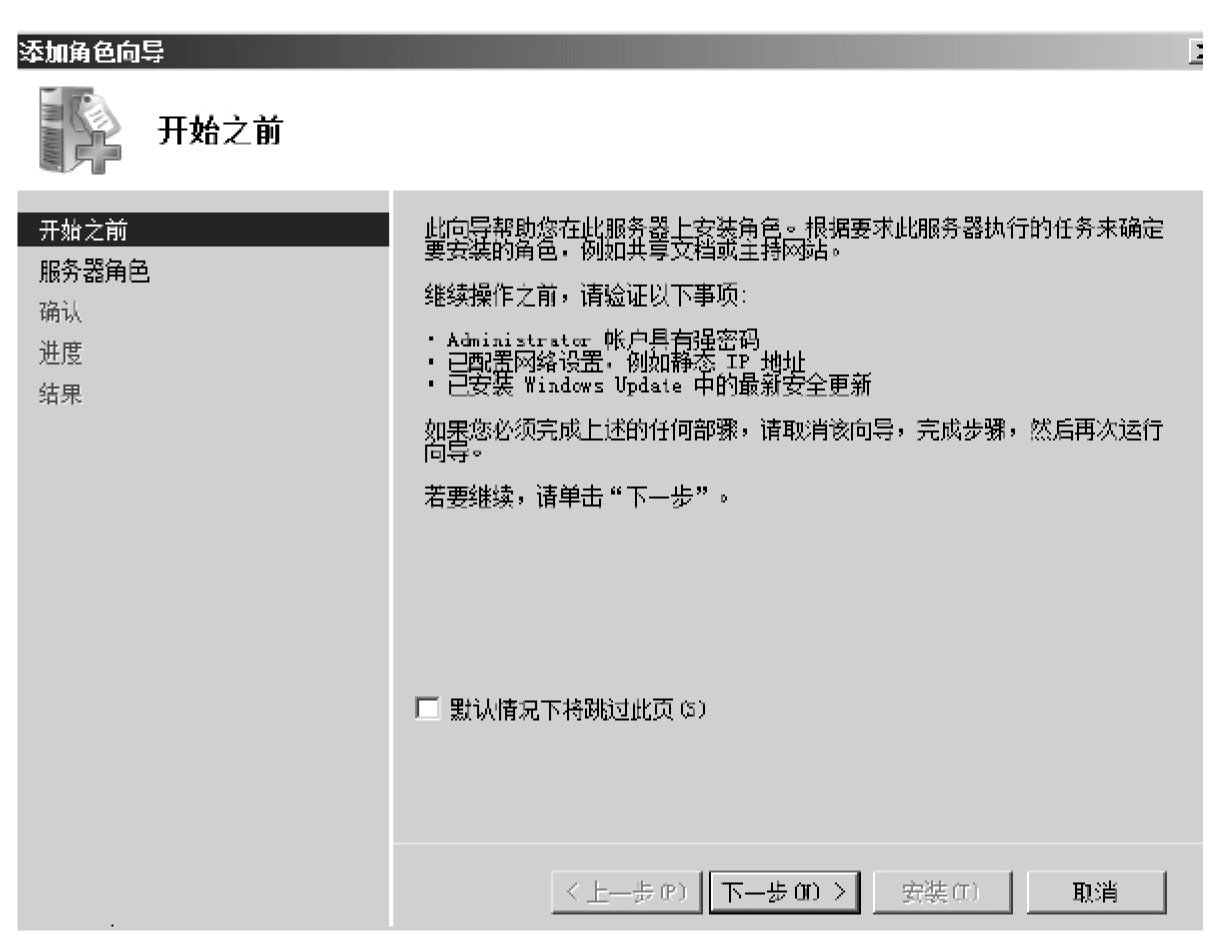


图 12-2　“添加角色向导”对话框

(3) 单击“下一步”按钮，打开如图 12-3 所示的“选择服务器角色”界面。单击选中“终端服务”复选框，单击“下一步”按钮。



图 12-3　选择“终端服务”

(4) 在如图 12-4 所示界面中，单击选中“终端服务器”对话框，两次单击“下一步”按钮。



图 12-4　选择“终端服务器”

(5) 如图 12-5 所示，选择身份验证方法，选择是否启用网络级别验证 NLA。NLA 可以在用户连接到终端服务器时对之进行网络级别的身份验证，提高了连接的安全性。单击“下一步”按钮。

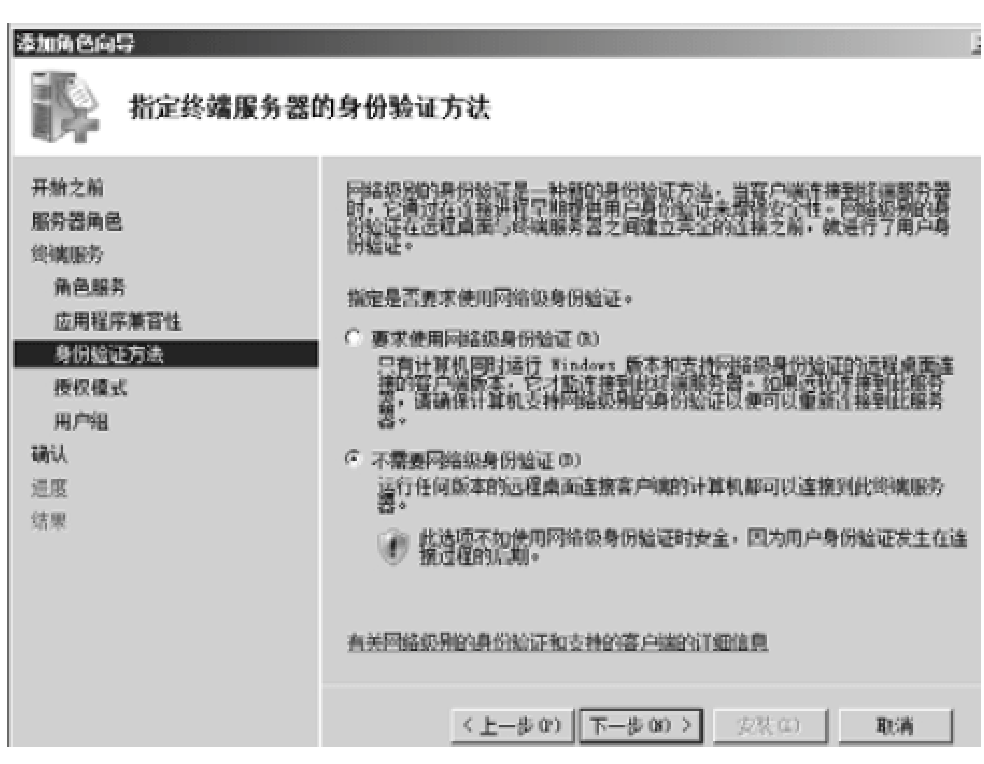


图 12-5　选择身份验证方法

注意：要启用 NLA 功能，还需要在服务器端的系统属性中，选择“只允许运行带网络级身份验证的远程桌面的计算机连接”，如图 12-6 所示。

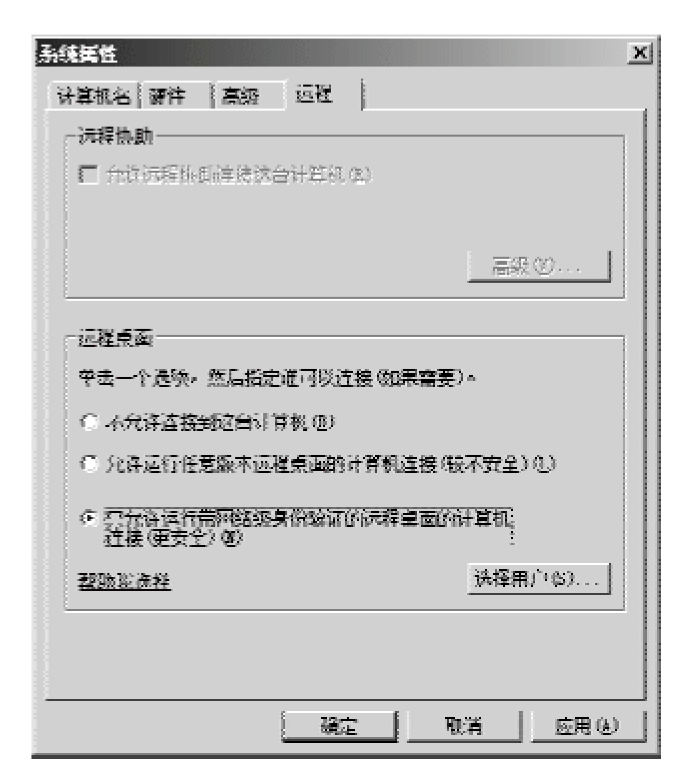


图 12-6　选择“只允许运行带网络级身份验证的远程桌面的计算机连接”

(6) 如图 12-7 所示，指定授权模式。使用终端服务器，必须对组织中部署的每台终端服务器拥有 Windows Server 2008 许可证，以及对访问终端服务器的设备拥有终端服务器客户端访问许可证(CAL)。对于正在运行的 Windows Server 2008 终端服务器，有以下两种终端服务器 CAL：每设备、每用户。选择哪个 CAL 取决于准备如何使用终端服务器。

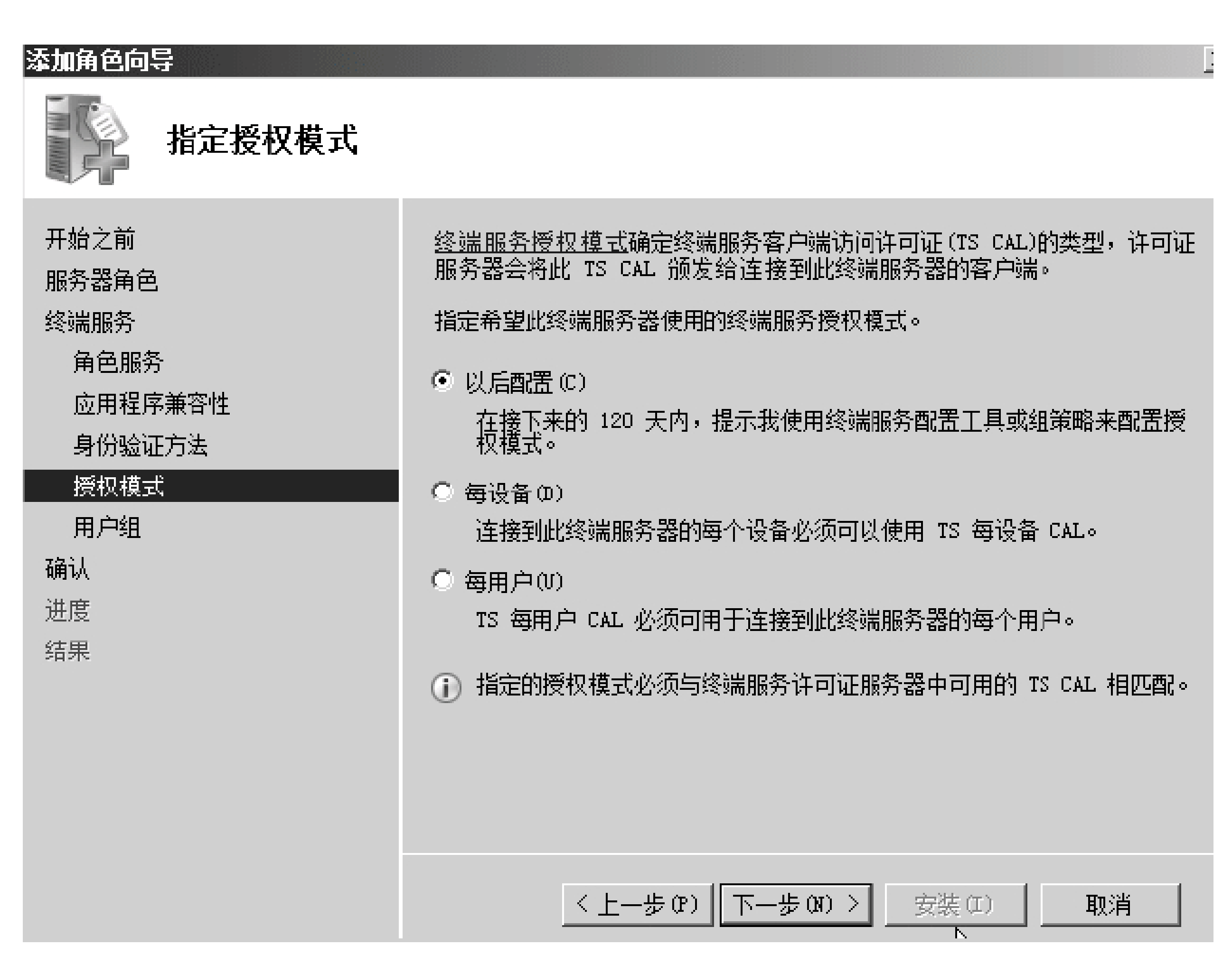


图 12-7　选择授权模式

如果使用每设备授权模式，并且客户端计算机或设备初次连接到终端服务器，默认情况下，向该客户端计算机或设备颁发一个临时证书。在客户端计算机或设备第二次连接到终端服务器时，如果许可证服务器已激活，并且有足够的 TS 每设备 CAL 可用，许可证服务器将向该客户端计算机或设备颁发一个永久 TS 每设备 CAL。选择每设备许可模式，管理用户拥有或控制的设备主桌面。如果不控制访问服务器的设备，不建议使用每设备许可模式，例如，网吧的计算机。

使用每用户许可模式，必须拥有每个用户的许可证。用户可从无数设备访问终端服务器，并且只需要一个 CAL(而不是适用于每个设备的 CAL)。

选择每用户许可模式，则执行下列操作：

- 为漫游用户提供访问；
- 为使用多台计算机的用户提供访问，例如便携式计算机和台式计算机；
- 为通过用户而不是计算机跟踪网络访问的组织提供轻松管理。

通常，如果组织拥有的计算机数多于用户数，每用户许可是一种经济有效的终端服务部署方法，因为只需支付用户访问终端服务器的费用，而不必支付用户访问终端服务器的每台设备的费用。

单击“下一步”按钮。

(7) 如图 12-8 所示，添加希望添加到 Remote Desktop Users 组中的任何用户或组，也可以今后再配置。单击“下一步”按钮。

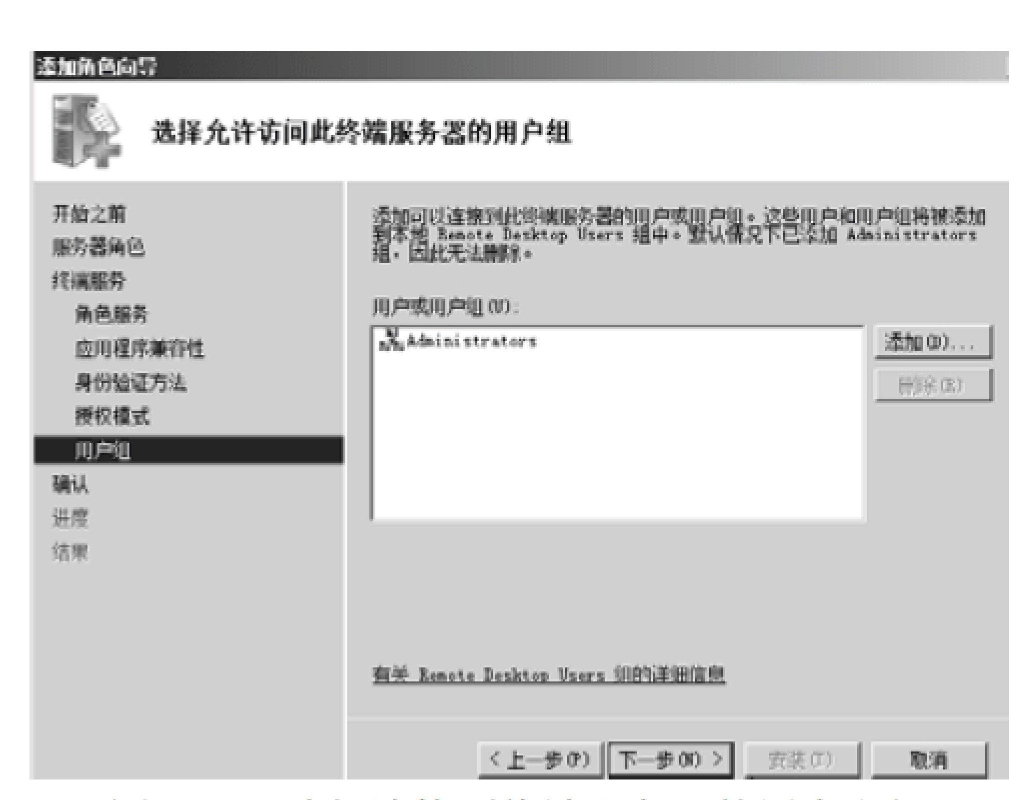


图 12-8　选择连接到终端服务器的用户和组

(8) 如图 12-9 所示，确认信息无误后，单击“安装”按钮。

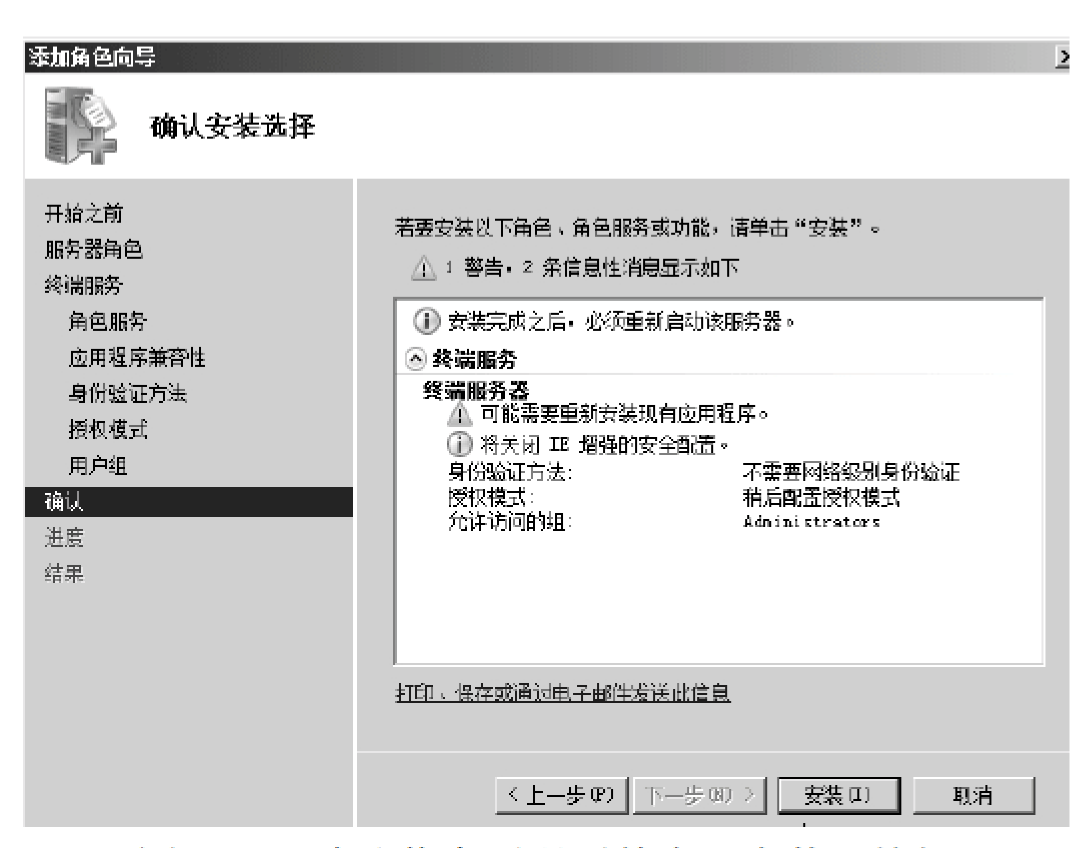


图 12-9　确认信息无误后单击“安装”按钮

(9) 之后，系统将提示重新启动服务器以完成安装过程。单击“关闭”按钮，然后单

击“是”按钮重新启动服务器。重新启动后，“继续配置向导”完成安装。当“安装结果”页面上出现“安装成功”消息时，单击“关闭”，如图 12-10 所示。

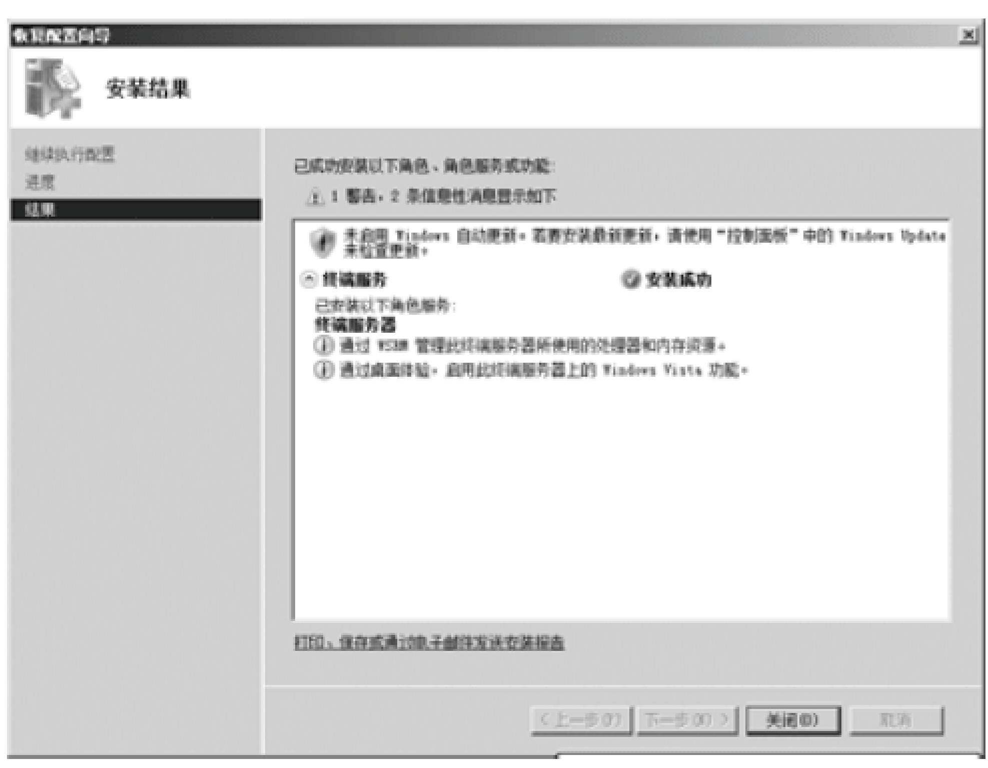


图 12-10　系统提示终端服务器安装成功

12.2　部署终端服务的客户端

在 Windows XP、Windows 2003 中部署终端服务，其客户端不需要进行太多的设置，只需要客户端具有远程桌面功能即可。远程桌面功能在 Windows 2000 Pro、Windows XP Pro 中均已经集成，在 Windows 98 客户端则需要单独进行安装。在 Windows 2008 中终端服务有了比较大的改进，用户可以通过 Web、远程桌面、终端服务器所创建的 rdp 或者 msi 文件进行连接。如果用户需要通过远程桌面进行连接，客户端需要安装远程桌面 6.0 以上版本。在 Vista 和 Windows 2008 以及 Windows XP SP3 中均已经整合远程桌面 6.0，Windows XP SP2 客户端用户可以通过微软网站下载安装。

操作步骤如下：

(1) 依次选择“开始”→“程序”→“附件”→“远程桌面连接”命令，可以打开“远程桌面连接”控制台，如图 12-11 所示，配置计算机名(或 IP 地址)和登录用户名。



图 12-11　配置远程桌面连接

(2) 单击“连接”按钮后，输入登录密码即可访问终端服务器。

12.3　部署终端服务应用程序

如果用户在同一台终端服务器上运行多个 RemoteApp 程序，RemoteApp 程序将共享同一个终端服务会话。

在 Windows Server 2008 中，用户可通过多种方式访问 RemoteApp 程序，具体取决于所选择的部署方法。用户可以执行以下任一操作：

- 使用终端服务 Web 访问(TS Web 访问)网站上该程序的链接。
- 双击由管理员创建并分发的远程桌面协议(.rdp)文件。
- 在桌面上，双击由管理员使用 Windows Installer(.msi)程序包创建并分发的程序图标，或从“开始”菜单的“程序”列表中直接选择。
- 双击扩展名与 RemoteApp 程序关联的文件。这可以由管理员使用 Windows Installer 程序包进行配置。

.rdp 文件和 Windows Installer 程序包都包含运行 RemoteApp 程序所需的设置。在本地计算机上打开 RemoteApp 程序之后，用户可以与正在终端服务器上运行的该程序进行交互，就好像它们在本地运行一样。

若要访问以.rdp 文件或 Windows Installer 程序包形式部署的 RemoteApp 程序，客户端计算机必须运行 Remote Desktop Connection(RDC)6.0 或 RDC 6.1。所支持的 RDC 客户端版本随 Windows Server 2008 和 Windows Vista 操作系统一起提供。若要为带 Service Pack 1 (SP1)的 Windows Server 2003 或带 Service Pack 2 (SP2)的 Windows XP 下载 RDC 6.0，若要通过 TS Web Access 访问 RemoteApp 程序，客户端计算机必须运行 RDC 6.1。RDC 6.1 随下列操作系统一起提供：

- Windows Server 2008
- 带 Service Pack1(SP1)的 Windows Vista
- 带 Service Pack 3(SP3)的 Windows XP

在安装完终端服务器角色服务后，在终端服务器上安装程序。如果使用 Windows Installer 程序包安装程序，该程序会自动在终端服务器安装模式下安装。如果要通过另一种安装程序包进行安装，请使用下列任一方法将服务器置于安装模式：

- 使用“控制面板”中的“在终端服务器上安装应用程序”选项来安装程序。
- 在安装程序之前，在命令提示符下，输入 change user/install。安装完程序之后，输入 change user/execute 退出安装模式。

如果程序相互关联或相互依存，建议将这些程序安装在同一台终端服务器上。例如，建议将 Microsoft Office 作为一个套件来安装，而不要将各个 Office 程序分别安装在不同的终端服务器上。

在下列情况下，应考虑将各个程序分别安装在不同的终端服务器上：

- 程序存在兼容性问题，可能会影响其他程序。
- 一个应用程序及若干关联用户可能会耗尽服务器的能力。

12.3.1　生成应用程序列表

步骤如下：

(1) 在如图 12-12 所示的服务器管理器窗口中，展开“角色”→“终端服务”左侧的“+”号，单击“TS RemoteApp 管理器”后，单击右侧窗口里的“添加 RemoteApp 程序”，打开“RemoteApp 向导”对话框，单击“下一步”按钮。



图 12-12　展开“角色”、“终端服务”

(2) 如图 12-13 所示，在“选择要添加到 RemoteApp 程序列表的程序”界面上，选中要添加到 RemoteApp 程序列表中的每个程序旁边的复选框，如 Microsoft Office Picture Manager，可以选择多个程序。

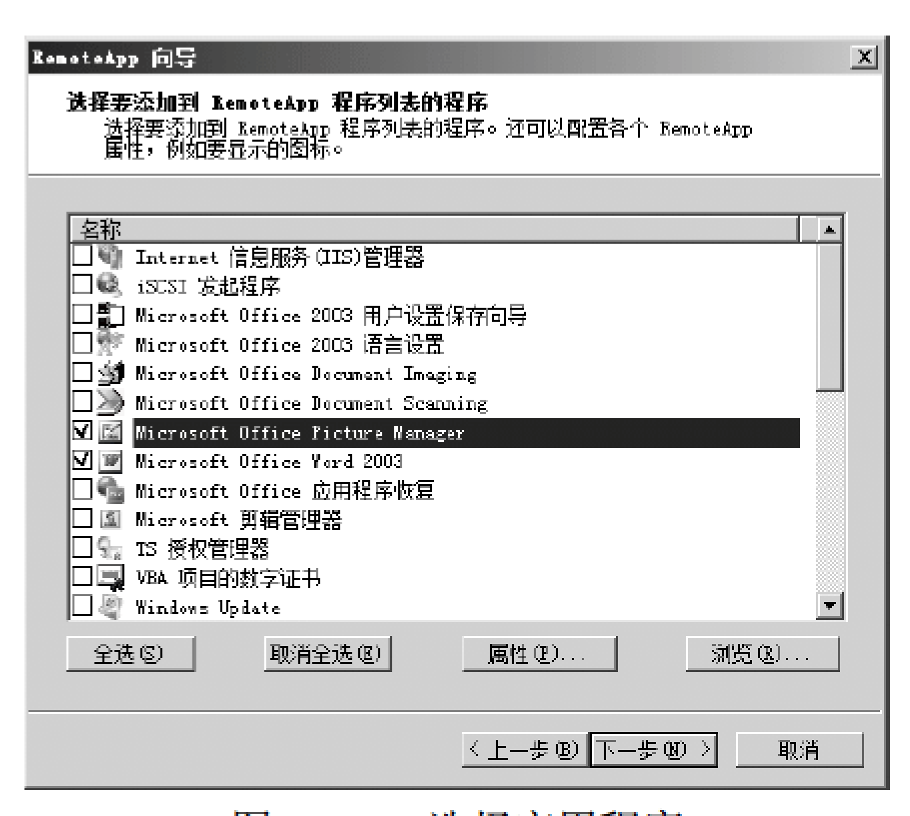


图 12-13　选择应用程序

注意：

① “选择要添加到 RemoteApp 程序列表的程序”页上显示的程序是终端服务器上所有用户“开始”菜单上出现的程序。如果要添加到“RemoteApp 程序”列表中的程序不在该列表中，则单击“浏览”按钮，然后为该程序指定.exe 文件的位置。

② 如果需要配置 RemoteApp 程序的属性，单击该程序名称，然后单击“属性”按钮，按照此步骤，参考如表 12-1 所示，设置表中列出的属性。

表 12-1　RemoteApp 程序属性

可以更改的属性	说明
将向用户显示的程序名	若要更改该名称，在“RemoteApp 程序名称”文本框中输入新名称
程序可执行文件的路径	若要更改该路径，在“位置”文本框中输入新路径，或单击“浏览”按钮 注：可以在路径名称中使用系统环境变量。例如，可以使用%windir%代替 Windows 文件夹的显式路径(例如 C:\Windows)。不能使用针对用户的环境变量
RemoteApp 程序的别名	别名是程序的唯一标识符，默认值为程序的文件名(不带扩展名)。建议不要更改此名称
RemoteApp 程序是否可通过 TS Web 访问获得	默认情况下，将启用“RemoteApp 程序可通过 TS Web 访问获得”设置。若要更改此设置，选中或取消该复选框
命令行参数	可以指定允许还是不允许命令行参数，或是否始终使用相同的命令行参数
程序图标	若要更改该图标，单击“更改图标”

程序属性设置完成后，单击“确定”按钮，然后单击“下一步”按钮。

(3) 单击“下一步”按钮，在出现的“复查设置”对话框中复查设置，单击“完成”按钮，出现如图 12-13 所示的窗口，所选的程序出现在 RemoteApp 程序列表中。

12.3.2　配置全局部署设置

可以配置应用于“RemoteApp 程序”列表中的所有 RemoteApp 程序的全局部署设置。这些设置应用于可通过 TS Web 访问获得的任意 RemoteApp 程序。此外，如果通过列出的任何 RemoteApp 程序来创建.rdp 文件或 Windows Installer 程序包，这些设置就是默认设置。

值得强调的是，使用 TS RemoteApp 管理器创建.rdp 文件或 Windows Installer 程序包时对部署设置所做的任何更改，会覆盖全局设置。

若要定义用户将如何连接到终端服务器(或终端服务器场)以访问 RemoteApp 程序，可以配置终端服务器部署设置。

1. 配置终端服务器设置

操作步骤如下：

(1) 打开“TS RemoteApp 管理器”，然后执行下列任一操作：在“操作”菜单中选择

“终端服务器设置”命令，或在“概述”窗格中，单击“终端服务器设置”旁边的“更改”按钮，如图 12-14 所示。



图 12-14　设置终端服务器

(2) 打开“终端服务器”选项卡，如图 12-15 所示，然后在“连接设置”中验证或修改服务器名称或场名称、远程桌面协议(RDP)端口号和服务器身份验证设置。

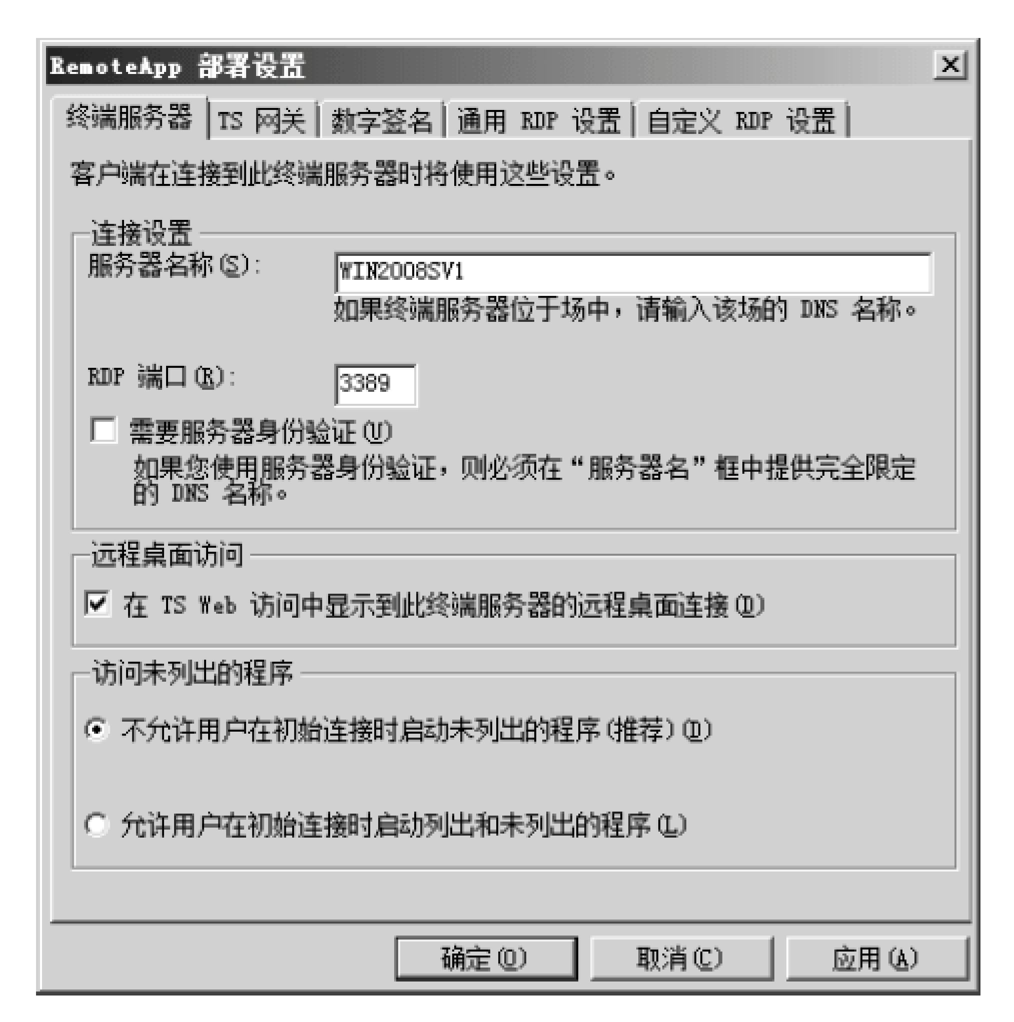


图 12-15　“终端服务器”选项卡

注意：如果选中了“需要服务器身份验证”复选框，则考虑下列事项：如果任何客户端计算机正在运行带 SP1 的 Windows Server 2003 或带 SP2 的 Windows XP，必须将终端服务器配置为使用安全套接字层(SSL)证书(不能使用自签名证书)。如果 RemoteApp 程序在 Intranet 中使用，并且所有客户端计算机均正在运行 Windows Server 2008 或 Windows Vista，则不必将终端服务器配置为使用 SSL 证书。在这种情况下，应使用网络级身份验证。

若要通过 TS Web 访问链接到完整的终端服务器桌面，在“远程桌面访问”中，选中“在 TS Web 访问中显示到此终端服务器的远程桌面连接”复选框。

在“访问未列出的程序”中，选择下列任一选项：

- 不允许用户在初始连接时启动未列出的程序(推荐)
- 允许用户在初始连接时启动列出和未列出的程序

注意：为了帮助防止恶意用户的攻击，或帮助防止用户在初始连接时无意中通过.rdp 文件启动程序，建议选择推荐的设置。推荐的设置不会阻止用户在使用 RemoteApp 程序连接到终端服务器之后，远程启动未列出的程序。例如，如果 Microsoft Word 在 RemoteApp 程序列表中，而 Microsoft Internet Explorer 浏览器不在该列表中，若用户启动远程 Word 会话，然后单击 Word 文档中的某个超级链接，可以启动 Internet Explorer。

如果选择不推荐的选项，用户可以在初始连接时通过.rdp 文件远程启动任何程序，而不仅仅是 RemoteApp 程序列表中的程序。为了帮助防止恶意用户的攻击，或帮助防止用户在初始连接时无意中通过.rdp 文件启动程序，建议不要选择第二种设置。

(3) 完成选择之后，单击“确定”按钮。

2. 配置终端服务网关设置

若要定义用户是否可以使用终端服务网关(TS 网关) 通过防火墙连接到终端服务器，可以配置 TS 网关部署设置。操作步骤如下：

(1) 打开“TS RemoteApp 管理器”，然后执行下列任一操作：在“操作”菜单中选择“TS 网关设置”命令，或在“概述”窗格中，单击“TS 网关设置”旁边的“更改”按钮。

(2) 在“TS 网关”选项卡上，配置所需的 TS 网关行为，如图 12-16 所示。可以配置自动检测 TS 网关服务器设置，还是使用指定的 TS 网关服务器设置，还是不使用 TS 网关服务器。

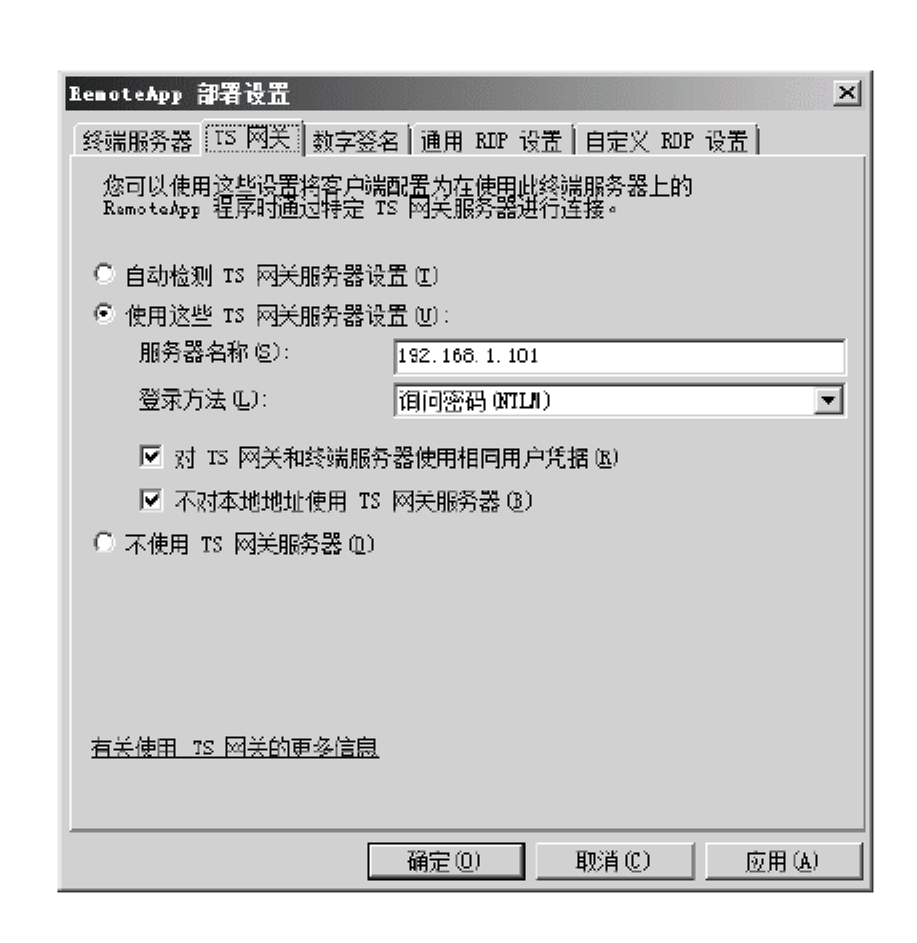


图 12-16　TS 网关配置

(3) 在 Windows 2008 环境中，Windows 2008 已配置为 TS 网关服务器以启用 Windows 远程工作网站功能。它也可以是其他终端服务器的 TS 网关。选择“使用这些 TS 网关服务器设置”。

配置 TS 网关服务器名称和登录方法,服务器名称必须和 TS 网关服务器的 SSL 证书中

指定的名称相匹配。

若要查找 Windows Server 2008 SSL 证书，在运行 Windows 2008 的服务器上，依次单击“开始”和“管理工具”。

(4) 单击“终端服务”，然后单击“TS 网关管理器”。

(5) 在“用户帐户控制”窗口中单击“继续”按钮。

(6) 在“TS 网管管理器”窗口的“TS 网关管理器”列表中，右键单击服务器名称，然后单击“属性”命令。

(7) 在“TS 网关服务器属性”对话框中，单击“SSL 证书”选项卡，然后记录“颁发给”中的服务器的名称。在终端服务器上使用此名称作为 TS 网关服务器名称。

如果希望连接尝试使用相同的用户凭据访问 TS 网关服务器和终端服务器，则选中“对 TS 网关和终端服务器使用相同用户凭据”复选框。但是，如果任何源(例如组策略设置)中存在冲突的凭据，并且这些凭据无法使用，用户仍可能会收到两次提供凭据的提示。如果连接使用默认凭据，并且这些凭据无法使用，用户也可能会收到两次提供凭据的提示。

如果希望客户端计算机自动检测何时需要 TS 网关，则选中“不对本地地址使用 TS 网关服务器”复选框。(选择此选项以优化客户端计算机的性能。)

若要对客户端连接始终使用 TS 网关服务器，则清除“不对本地地址使用 TS 网关服务器”复选框。

(8) 单击“确定”按钮。

3. 配置数字签名设置

可以使用数字签名为用于将 RemoteApp 连接到终端服务器的.rdp 文件签名。包括用于通过 TS Web 访问连接到终端服务器上的 RemoteApp 程序和终端服务器桌面的.rdp 文件。若要使用已进行数字签名的.rdp 文件连接到 RemoteApp 程序，客户端计算机必须正在运行 RDC 6.1(客户端支持远程桌面协议 6.1)。

如果使用数字证书，连接文件上的加密签名将提供有关作为其发布者的身份的可验证信息。这样，客户端计算机便可将用户所在的组织视为 RemoteApp 程序或远程桌面连接的来源，然后启动或禁止基于信任条件的连接。这样可以防止使用恶意用户已篡改的.rdp 文件。

通过使用服务器身份验证证书(SSL 证书)或代码签名证书，可以为用于 RemoteApp 连接的.rdp 文件签名。可以从公用证书颁发机构(CA)或您的公钥基础结构层次结构中的某个企业 CA 获取 SSL 证书和代码签名证书。

如果已在对终端服务器连接或 TS 网关连接使用 SSL 证书，可以使用同一个证书为.rdp 文件签名。在 Windows 2008 环境中，TS 网关已安装在运行 Windows 2008 并具有 SSL 证书签名的服务器上。

配置数字签名设置的操作步骤如下：

(1) 从 Windows Server 2008 导出终端服务网关证书。步骤包括：

① 在运行 Windows 2008 的服务器上，依次单击“开始”和“管理工具”。

② 单击“终端服务”，然后单击“TS 网关管理器”。

③ 在“TS 网管管理器”窗口的“TS 网关管理器”列表中，右键单击服务器名称，然后单击“属性”命令，如图 12-17 所示。



图 12-17　“终端服务器”选项卡

④ 在“TS 网关服务器属性”对话框中，依次单击“SSL 证书”选项卡和“浏览证书”。

⑤ 在“安装证书”对话框的“证书”列表中，单击当前已安装的证书，然后单击“查看证书”。

⑥ 在“证书”对话框中，依次单击“详细信息”选项卡和“复制到文件”。

⑦ 在证书导出向导中，单击“下一步”按钮。

⑧ 确认选中了“是，导出密钥”，然后单击“下一步”按钮。确认选中了“包括证书路径中的所有证书(如果可能)”和“导出所有扩展属性”，然后单击“下一步”按钮。请不要选中“如果导出成功，删除密钥”。

⑨ 输入用于保护证书文件的强密码，然后单击“下一步”按钮。

若要保存.pfx 文件(例如，C:\trustedcert.pfx)，请选择只有管理员可以访问的安全位置，然后单击“下一步”按钮。完成此向导。

(2) 导入 SSL 证书到终端服务器。步骤包括：

① 使用网络或 USB 驱动器将 trustedcert.pfx 文件移动到其他终端服务器。在其他终端服务器上，双击.pfx 文件。

② 在证书导入向导的“欢迎使用”页上，单击“下一步”按钮。

③ 浏览到已保存的.pfx 文件的位置，然后单击“下一步”按钮。

④ 输入在导出过程中输入的密码，确认选中了“标志此密钥为可导出的密钥”和“包括所有扩展属性”，然后单击“下一步”按钮。

⑤ 在“证书存储”页上，选中“将所有的证书放入下列存储”，依次单击“浏览”和“个人”。单击“下一步”按钮，即完成此向导。

⑥ 接着，配置在 RemoteApp 中使用的数字证书。步骤如下：

⑦ 打开“TS RemoteApp 管理器”，然后执行下列任一操作：在“操作”菜单中选择“数字签名设置”命令，或在“概述”窗格中，单击“数字签名设置”旁边的“更改”按钮。

⑧ 选中“使用数字证书签名”复选框。

⑨ 在“数字证书详细信息”对话框中，单击“更改”。

⑩ 在“选择证书”对话框中，单击要使用的证书，然后单击“确定”按钮。

“选择证书”对话框由本地计算机的证书存储区或个人证书存储区中的证书填充。要使用的证书必须位于这两个存储区的任一存储区中；如果用户从公用计算机或家用计算机连接到 RemoteApp 程序，必须使用作为“Microsoft 根证书程序成员”之一的公共证书颁发机构(CA)发放的 CA 证书，或者使用由作为“Microsoft 根证书程序成员”之一的公共 CA 共同签名的企业 CA 发放的证书。

如果用户正使用自行颁发的证书，那么必须为远程计算机上的服务器安装安全证书。只应从直接连接到组织网络的计算机下载证书安装程序包。请勿通过 Internet 下载此程序包。

(3) 为远程计算机上的服务器安装安全证书。步骤如下：

① 从 Windows 2008 网络中的计算机中，打开 Web 浏览器并在地址栏中输入以下地址：\\服务器名称\public\downloads(服务器名称是正在运行 Windows 2008 的服务器的名称)。

② 将文件 Install Certificate Package.zip 复制到便携存储介质(例如 CD 或 USB 驱动器)上。

③ 将 CD 或 USB 驱动器插到未加入 Windows 域且您希望通过它访问远程工作网站的计算机中。

④ 在 Windows 浏览器中，导航至用户将 Install Certificate Package.zip 复制到的位置。

⑤ 右击 Install Certificate Package.zip，然后单击“全部提取”命令。

⑥ 在“提取压缩(Zipped)文件夹”对话框中，输入用户希望将文件提取到的文件夹位置，然后单击“提取”按钮。

⑦ 打开已提取文件所在的文件夹，然后双击 InstallCertificate。

⑧ 选择“将此证书安装在计算机上”，然后单击“安装”按钮。

12.3.3 部署 RemoteApp 到用户

可以使用下列任一部署方法：

- 通过共享文件夹或其他分发机制(例如，Microsoft Systems Management Server 或 Active Directory 软件分发)将 RemoteApp 程序作为.rdp 文件或 Windows Installer 程序包进行分发。
- 通过 TS Web 访问分发 RemoteApp 程序，在网站上获取 RemoteApp 程序。

下面介绍最常用的通过 TS Web 访问部署 RemoteApp 程序。

使用 TS Web 访问，用户可从 Internet 上的网站或从 Intranet 访问 RemoteApp 程序。若要启动 RemoteApp 程序，请用户单击“程序”图标。TS Web 访问提供了一种涉及少配置的解决方案。默认的 TS Web 访问页包括可集成到自定义网页的自定义 Web 部件。

若要使用 TS Web 访问部署 RemoteApp 程序，操作如下：

- 安装 TS Web 访问角色服务。
- 填充 TS Web 访问计算机安全组。
- 为 TS Web 访问指定可访问的终端服务器 RemoteApp 程序列表。

1. 安装 TS Web 访问角色服务

必须是本地 Administrators 组的成员才能完成此步骤。必须在希望用户通过 Web 连接以访问 RemoteApp 程序的服务器上安装 TS Web 访问角色服务。在安装 TS Web 访问角色服务时，还会安装 Microsoft Internet Information Services (IIS) 7.0。

安装 TS We 访问的服务器 We 服务器。该服务器不必是终端服务器。在 Windows 2008 网络中，建议在安装了终端服务的同一服务器或 Windows 域内的任何其他服务器(但不要在运行 Windows 2008 的服务器)上安装 TS Web 访问。

(1) 打开服务器管理器：选择“开始”→“管理工具”→“服务器管理器”命令。

(2) 如果已安装“终端服务”角色，执行下列操作：在“角色摘要”下，单击“终端服务”；在“角色服务”中，单击“添加角色服务”；如图 12-18 所示，在“选择角色服务”页上，选中“TS Web 访问”复选框。

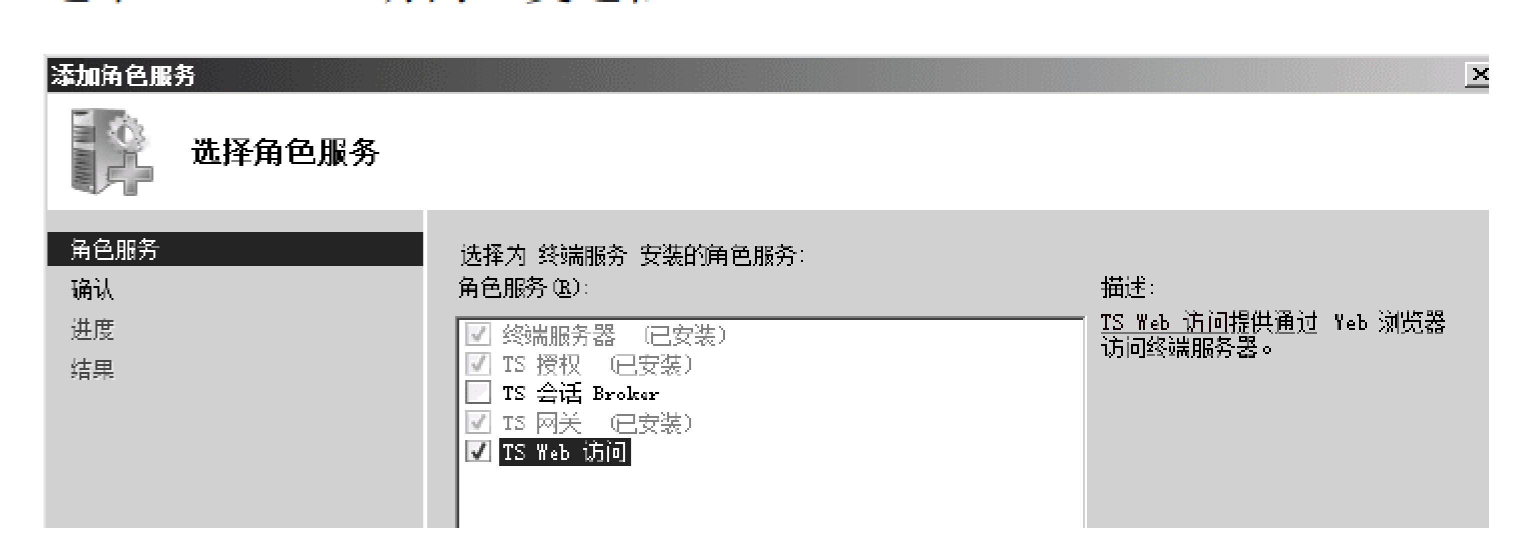


图 12-18　选中“TS Web 访问”复选框

如果尚未安装“终端服务”角色，请执行下列操作：在“角色摘要”，单击“终端服务”；在“开始之前”页上，单击“下一步”按钮；在“选择服务器角色”页上，选中“终端服务”复选框，然后单击“下一步”按钮；复查“终端服务”页，然后单击“下一步”按钮；在“选择角色服务”页上，选中 TS Web 访问复选框。

(3) 复查必需的角色服务相关信息，然后单击“添加必需的角色服务”。单击“下一步”按钮。

(4) 复查“Web 服务器(IIS)”页，然后单击“下一步”按钮。

(5) 在“选择角色服务”页上，提示选择要为 IIS 安装的角色服务。单击“下一步”按钮。

(6) 在“确认安装选择”页上，单击“安装”按钮，接下来进入安装进程，如图 12-19 所示。



图 12-19　安装“TS Web 访问”

(7) 在“安装结果”页上，确认安装已成功，然后单击“关闭”按钮。

2. 填充 TS Web 访问计算机安全组

如果 TS Web 访问服务器和托管 RemoteApp 程序的终端服务器是不同的服务器，则必须将 TS Web 访问服务器的计算机帐户添加到终端服务器上的 TS Web 访问计算机安全组中。

将 TS Web 访问服务器的计算机帐户添加到该安全组中，执行下列操作：

(1) 在终端服务器上，依次选择“开始”→“管理工具”→“计算机管理”命令。

(2) 在“用户帐户控制”窗口中单击“继续”。

(3) 在控制台窗格中，展开“本地用户和组”，然后单击“组”。

(4) 在详细信息窗格中，双击“TS Web 访问计算机”。

(5) 在“TS Web 访问计算机属性”对话框中，单击“添加”按钮。

(6) 在“选择用户、计算机或组”对话框中，单击“对象类型”。

(7) 在“对象类型”对话框中，选中“计算机”复选框，然后单击“确定”按钮。

(8) 在“输入要选择的对象名称”框中，输入 TS Web 访问服务器的计算机帐户，然后单击“确定”按钮。

(9) 单击“确定”按钮，关闭“TS Web 访问计算机属性”对话框。

3. 为 TS Web 访问指定可访问的终端服务器 RemoteApp 程序列表

可以将 TS Web 访问配置为填充指定的终端服务器或终端服务器场的 Web 部件中出现的 RemoteApp 程序列表。

(1) 为 TS Web 访问指定数据源。

默认情况下，TS Web 访问会填充来自单个终端服务器的 RemoteApp 程序列表，并指向本地主机。为 RemoteApp 程序列表中的 TS Web 访问启动的所有 RemoteApp 程序填充终端服务器的 Web 部件。

若要完成此步骤，必须使用本地 Administrator 帐户或作为 TS Web 访问服务器上的 TS Web 访问 Administrators 组成员的帐户登录 TS Web 访问服务器。请按照此列表中的步骤操作。

若要指定要充当数据源的终端服务器，请执行下列操作：

① 连接到 TS Web 访问网站。按下列步骤执行：在 TS Web 访问服务器上，选择“开始”→“管理工具”→“终端服务”→“TS Web 访问管理”命令。

然后，使用 Internet Explorer 连接到 TS Web 访问网站。默认情况下，该网站位于以下地址，其中服务器名称是 TS Web 访问服务器的名称：http://服务器名称/ts

② 用本地 Administrator 帐户或作为本地 TS Web 访问 Administrators 组成员的帐户登录到站点(如果已使用其中任一帐户登录到该计算机，系统不会提示用户输入凭据)。

③ 如果使用“TS Web 访问管理”选项访问 TS Web 访问站点，该页将自动打开至“配置”选项卡。在“配置”选项卡的“编辑器区域”区域的“终端服务器名称”框中，输入要充当数据源的终端服务器的名称。

④ 单击“应用”按钮。

(2) 接到 TS Web 访问。

默认情况下，可以访问以下位置的 TS Web 访问网站，其中服务器名称是安装了 TS Web 访问的 Web 服务器的 NetBIOS 名称或完全限定的域名：

http://服务器名称/ts

如果通过公用计算机(例如网吧中的计算机)连接到 TS Web 访问，应清除 Web 部件右下角显示的“我使用的是符合组织安全策略的专用计算机”复选框。在公用模式下，不会提供保存凭据的选项，也不启用位图的缓存。

12.3.4 生成客户端程序

有 3 种方式可以使客户端来运行应用程序列表中的程序：(1)添加.rdp 文件；(2)制作 Windows 安装包；(3)web 访问。这里介绍前两种方法。

1. 通过 RemoteApp 程序创建.rdp 文件

可以使用 RemoteApp 向导，通过“RemoteApp 程序”列表中的任意程序创建.rdp 文件。步骤如下：

(1) 选择“开始”→“管理工具”→“终端服务”→“TS RemoteApp 管理器”命令，启动 TS RemoteApp 管理器。

(2) 在“RemoteApp 程序”列表中，单击要为其创建.rdp 文件的程序，若要选择多个

程序，按住 Ctrl 键并单击每个程序名。如果选择了多个程序，此过程剩余部分所述的设置应用于所有所选的程序。为每个程序分别创建一个.rdp 文件。右击选择的应用程序，单击“创建.rdp 文件”，如图 12-20 所示。



图 12-20　创建.rdp 文件

在出现的窗口中连续两次单击“下一步”按钮，出现如图 12-21 所示窗口，单击“完成”按钮。



图 12-21　单击“完成”按钮

(3) 在“指定程序包设置”页上，执行下列操作：

① 在“输入要保存程序包的位置”框中，接受默认位置，或单击“浏览”指定.rdp 文件的新位置。

② 在“终端服务器设置”区域，单击“更改”修改服务器名称、RDP 端口号和需要服务器身份验证设置。完成操作后，单击“确定”按钮。

③ 在“TS 网关设置”区域，单击“更改”修改或配置客户端计算机是否将使用 TS 网关服务器跨防火墙连接到目标终端服务器。完成操作后，单击“确定”按钮。

④ 若要为.rdp 文件进行数字签名，在“证书设置”部分，单击“更改”选择或更改要使用的证书。选择要使用的证书，然后单击“确定”按钮。

(4) 完成后，单击“下一步”按钮。

(5) 在“复查设置”页上，单击“完成”按钮。

向导完成后，保存.rdp 文件的文件夹将在新窗口中打开。可以确认存在.rdp 文件。

2. 通过 RemoteApp 程序创建 Windows Installer 程序包

可以使用 RemoteApp 向导，通过“RemoteApp 程序”列表中的任意程序创建 Windows Installer (.msi)程序包。操作步骤如下：

(1) 在图 12-12 中，选择一个或多个程序(如果选择了多个程序，此过程剩余部分所述的设置应用于所有所选的程序，为每个程序分别创建一个 Windows Installer 程序包)后，右击选择的应用程序，在弹出的菜单中单击“创建 Windows Installer 程序包”，类似如上步骤可创建 Windows Installer 程序包。如图 12-22 窗口中，复制.rdp 文件或 Windows Installer 程序包到客户端。

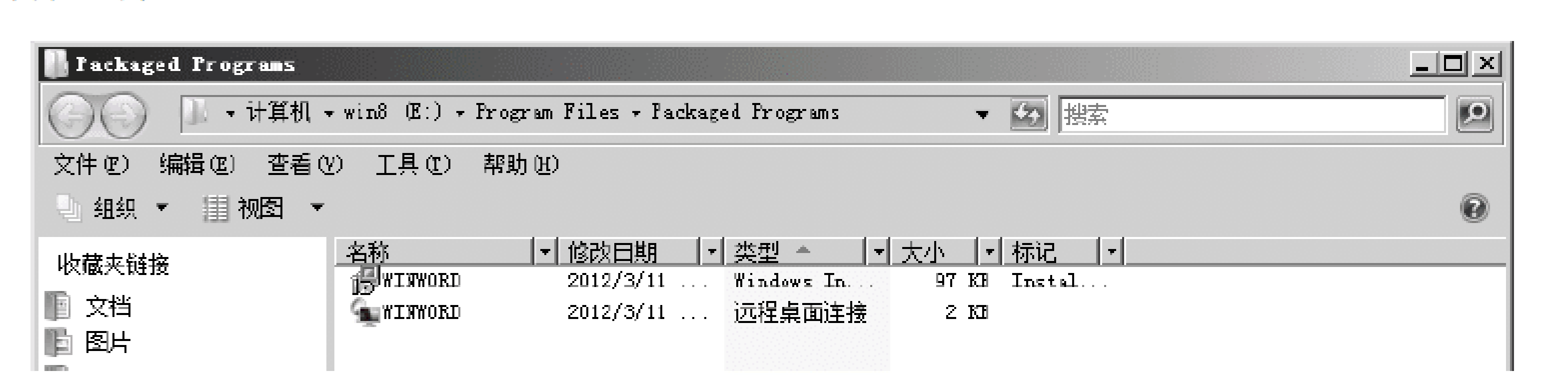


图 12-22　生成的.rdp 文件、Windows Installer 程序包

(2) 在“欢迎使用 RemoteApp 向导”页上，单击“下一步”按钮。

(3) 在“指定程序包设置”页上，执行下列操作：

① 在“输入要保存程序包的位置”框中，接受默认位置，或单击“浏览”指定 Windows Installer 程序包的新位置。

② 在“终端服务器设置”区域，单击“更改”修改服务器名称、RDP 端口号和需要服务器身份验证设置，完成操作后单击“确定”按钮。

③ 在“TS 网关设置”区域，单击“更改”修改或配置客户端计算机是否将使用 TS 网关服务器跨防火墙连接到目标终端服务器。(有关这些设置的详细信息，请参阅本文档的“配置全局部署设置”部分的“配置 TS 网关设置”)完成操作后，请单击“确定”按钮。

④ 若要为.rdp 文件进行数字签名，在“证书设置”部分，单击“更改”选择或更改要使用的证书。选择要使用的证书，然后单击“确定”按钮。

(4) 完成后，单击“下一步”按钮。

(5) 在“配置分发程序包”页上执行下列操作：①在“快捷方式图标”区域，指定该

程序的快捷方式图标在客户端计算机上的显示位置。②在“接管客户端扩展”区域，配置是否接管该程序的客户端文件扩展名。

如果将客户端计算机上的文件扩展名与 RemoteApp 程序关联，对于终端服务器上由该程序处理的所有文件扩展名，在客户端计算机上也与 RemoteApp 程序关联。例如，如果将 Microsoft Word 作为 RemoteApp 程序添加并配置此选项以接管客户端文件扩展名，那么由该 Word 接管的客户端计算机上的任意文件扩展名都与远程 Word 关联。这意味着客户端计算机上现有的任何程序不再处理文件扩展名(例如.doc 和.dot)。注意，系统不会提示用户终端服务器是否应接管该程序的文件扩展名。

若要查看与终端服务器上的某个程序关联的文件扩展名，依次单击“开始”、“控制面板”，然后双击“默认程序”。单击“将文件类型或协议与程序关联”，以查看文件扩展名及其默认关联的程序。

若要查看与终端服务器上的某个程序关联的文件扩展名，依次单击“开始”、“控制面板”，然后双击“默认程序”。单击“将文件类型或协议与程序关联”，以查看文件扩展名及其默认关联的程序。

不要在终端服务器上安装启用此设置时创建的 Windows Installer 程序包。如果这样做，使用 Windows Installer 程序包的客户端计算机可能无法启动关联的 RemoteApp 程序。

(6) 配置了分发程序包的属性之后，单击“下一步”按钮。

(7) 在“复查设置”页上，单击“完成”按钮。

向导完成后，保存 Windows Installer 程序包的文件夹将在新窗口中打开。可以确认存在 Windows Installer 程序包。

12.4　配置客户端应用环境

若要连接到 TS Web 访问，客户端计算机必须运行 RDC 6.1。RDC 6.1 随下列操作系统一起提供：

- Windows Server 2008
- 带 Service Pack1(SP1)的 Windows Vista
- 带 Service Pack 3(SP3)的 Windows XP

此外，必须启用终端服务 ActiveX 客户端控件。该 ActiveX 控件随 RDC 6.1 一起提供。

如果客户端计算机正运行 Windows Server 2008 或带 SP1 的 Windows Vista，并且收到 Internet Explorer 信息栏上显示的该站点限制显示某些内容的警告消息，依次单击消息行上的“禁用的加载项”和“运行 ActiveX 控件”。您可能会看见一条安全警告。需确保 Microsoft Corporation 是 ActiveX 控件的发行者，然后单击“运行”按钮。

注意：

如果该 Internet Explorer 信息栏没有出现，并且不能连接到 TS Web 访问，客户端用户

可以使用 Internet Explorer 的“工具”菜单上的“管理加载项”工具来启用终端服务 ActiveX 控件。加载项显示为 Microsoft 终端服务客户端控件。

如果客户端计算机正运行带 SP3 的 Windows XP，当用户首次访问 TS Web 访问站点时，该网站的页面显示一条错误消息，指出“ActiveX 控件未安装或未启用”。使用下列步骤启用 ActiveX 控件(以在带 SP3 的 Windows XP 中启用 ActiveX 控件为例)：

(1) 连接到 TS Web 访问站点，然后输入用户的登录凭据。

(2) 根据正运行的 Internet Explorer 的版本，执行下列操作之一：

如果客户端计算机正使用 Internet Explorer7，在“工具”菜单上依次单击“管理加载项”和“启用或禁用加载项”命令。

如果客户端计算机正使用 Internet Explorer 6，在“工具”菜单上单击“管理加载项”命令，如图 12-23 所示。



图 12-23　在“工具”菜单上单击“管理加载项”命令

此时将出现“管理加载项”对话框。请确保将“显示”列表设置为“Internet Explorer 中当前加载的加载项”。

(3) 在“已禁用”中，单击“Microsoft 终端服务客户端控件(redist)”或“Microsoft RDP 客户端控件(redist)”，已列出其中之一。

(4) 在“设置”中，单击“启用”按钮。(如果正运行 Internet Explorer 6，在对话框中单击“确定”，该对话框指出您可能需要重新启 Internet Explorer，更改才会生效)。如果 ActiveX 控件列出两次，那么两个实例都启用。

(5) 单击“确定”按钮关闭“管理加载项”对话框(如果正运行 Internet Explorer 7，在对话框中单击“确定”按钮，重新启动 Internet Explorer，更改才会生效)。

12.5　客户端访问 TS 的应用程序

将.rdp 文件复制到客户端计算机。在客户端计算机，双击打开.rdp 文件，输入登录密码，可打开终端服务器上的应用程序。

12.6　本章小结

本章介绍了终端服务器及其客户端的配置，包括应用程序在终端服务器、客户端的配置和应用。掌握此技术，对于提高 Windows 网络的资源共享效率大有裨益。

12.7　思考与练习

【思考题】

1. 什么是终端服务？其实现原理是什么？
2. 终端服务的主要部署步骤有哪些？

【练习题】

部署和运用终端服务的应用程序(参考 12.3～12.5 节)。

第13章　代理服务

【本章导读】

通过 Windows Server 2008 及其相关软件配置的网络服务器还能为内网用户起到代理上网的作用，即用户通过 Windows Server 2008 服务器能访问外网的资源。Windows Server 2008 服务器又是一种特殊的防火墙，在提供代理上网服务的同时能保护内网用户及其资源免受来自外网的侵害。通过与 Forefront TMG(可简称为“TMG”)的集成，Windows Server 2008 服务器能够发挥代理服务器的作用。

13.1　TMG 概述

微软发布的 ISA Server 新一代版本 Forefront Threat Management Gateway(安全威胁管理网关)，一般称为 Forefront TMG，包括如下组件：

- 安全配置和企业级集中管理控制台：Forefront Server Security Management Console；
- 端点防护：Forefront Client Security(FCS)；
- 信息协作防护：Forefront Security for Exchange Server(FSE)and Forefront Security for SharePoint(FSSP)；
- 边缘防护：Forefront Threat Management Gateway(Forefront TMG)。

13.1.1　TMG 功能简介

目前 Forefront TMG、NAP、Forefront Endpoint Protection 的客户端仍然是独立的；在不久的将来，可能就只有一个客户端来实现这所有的功能。这样可以极大地简化 IT 管理，同时通过集成技术，也可以实现更为完美、便捷的安全管控。

Forefront TMG 就是统一的威胁管理网关，顾名思义 TMG 所提供的是全面的企业网络安全防护能力。它是微软具有划时代意义的企业级网络安全产品。这种意义主要体现在以下几个方面。

1. 企业级的安全整合与管理

从 2006 年开始，微软把主要的安全产品整合在一个产品系列 Forefront 中。在 Forefront 产品系列中，ISA 主要负责网络边缘范围的安全防范与保护。但是，和其他防火墙产品不同，ISA 不仅仅是一个防火墙，而是通过与其他微软产品或技术(例如活动目录)结合来实现完善的企业安全管理与控制。微软从 ISA(互联网安全与加速，Internet Security and

Acceleration)变更到 TMG(安全威胁管理网关，Threat Management Gateway)就可以看出，微软不仅仅只想负责网络边缘的安全与防护，而是想实现统一的企业安全威胁管理，这也表现出了微软在企业安全领域的决心。

TMG 是作为新一代的 Forefront 产品系列 Stirling 的重要组成部分，完整的 Stirling 套件包括 Forefront Protection Manager、Forefront Endpoint Protection 2010、Forefront Protection 2010 for Exchange/Sharepoint 和 Forefront TMG 这五个独立组件，并且可以融合其他的一些安全产品或技术，例如 NAP 或者第三方技术或者产品等等。在 Forefront Stirling 产品系列中，其中一个最为重大的新特性就是基于 Forefront Stirling 的 Security Assessment Sharing(SAS)功能，可以在全系列的 Forefront Stirling 产品中进行安全评估信息的共享。SAS 相当于在 Stirling 各个组件之间构建了一个信息共享的通道，在这个通道中，所有组件共享彼此的安全评估信息，例如某个计算机是否有中病毒的嫌疑，某个用户访问是否是恶意访问，并且基于这个安全评估信息，执行特定的操作。这样带来的好处就是 Stirling 所有组件之间都是协同工作的，具有安全联动响应的特性。例如 Forefront Endpoint Protection 发现计算机中毒了，那么这个安全评估信息就直接通过 SAS 发送给 TMG 和 Protection for Exchange，TMG 就可以直接拒绝来自该计算机的访问，而 Protection for Exchange 就可以扫描该计算机上当前登录用户的邮箱等等。

另外，在 TMG 中，除了一贯的提供对于活动目录的支持外，TMG 已经能够完美的和 NAP 进行集成，实现完善的 VPN 隔离与控制。

2. 架构变更与提升

由于 ISA Server 2004/2006 的性能基本上到了 Windows Server 2003 的极限，因此 ISA Server 2006 和 ISA Server 2004 相比，性能基本没有太大的提升。TMG 最显著的特性，就是从 32 位的 Windows Server 2003 架构完美地迁移到 64 位的 Windows Server 2008/2008 R2 的架构，也不再提供针对 Windows Server 2003 和 32 位操作系统的支持。

3. Web 非法软件扫描与过滤

经过微软长期的分析与研究，发现在非法软件如病毒、蠕虫、间谍软件等的传播途径中，基于 Web 的传播方式是最为流行、也最为广泛的一种。因此作为 TMG 的一个重要创新，微软新增了针对 HTTP/HTTPS 传输内容的 Web 非法软件扫描功能，以及针对 URL 地址类别进行访问控制的功能。

(1) HTTP 非法软件扫描

TMG 中内置的 Web 非法软件扫描引擎为新一代的 Forefront Endpoint Protection 反病毒引擎，并且通过 Microsoft Update 来实现特征定义的更新。在 Web 非法软件扫描功能配置中，可以配置是否进行 Web 非法软件扫描、哪些站点不进行扫描、当发现病毒时是否尝试清除病毒、当处理时间超过多少就拒绝访问、当压缩文件嵌套多少层就拒绝访问、当文件大小超过多少就拒绝访问等。

(2) HTTPS 扫描

HTTPS 是加密的 HTTP 传输，标准的传输端口为 TCP 443。由于 HTTPS 加密传输的特性，传输内容不可知，导致很多的非法软件例如木马使用 HTTPS 协议来进行传输，甚至不使用标准的 HTTPS 协议，仅使用 TCP 443 端口来进行传输，这样看起来就像是 HTTPS 协议传输。但是由于绝大部分防火墙包括硬件和软件缺乏针对 HTTPS 传输内容的访问控制，因此只能开放 TCP 443，导致企业网络的安全性得不到有效的保障。

在 Forefront TMG 中，提供了针对 HTTPS 传输内容的扫描检查功能，因此可以阻止病毒、木马、间谍软件等非法软件通过 HTTPS 协议来实现传播，提高企业网络的整体安全性。

(3) URL 地址类别过滤

在微软内部，具有一个安全服务，叫做 Microsoft Reputation Services。这个 MRS 服务实际上是一个整合了来自大量合作伙伴所提供数据的数据库。在这个数据库中存放的数据就是全球 Web 站点的相关类别及安全评估信息，例如某个 URL 地址是否是一个恶意站点，以及这个 URL 地址的类别是新闻站点、体育站点还是娱乐站点之类的信息。

在 TMG 中，就可以基于 MRS 数据库的分类，对用户的访问行为进行控制。在 TMG 中包含 91 个 URL 地址类别，可以根据需要的类别来阻止或允许用户访问。

4. 路由架构改进

在 TMG 中，针对路由架构和底层传输同样进行了大规模的改进，主要包括 ISP-R 传输链路冗余、增强的 NAT 转换、SIP 协议支持等。

5. 网络入侵保护系统

在 TMG 中，第一次引入了微软自行研发的网络入侵保护系统(NIS)。这个网络入侵保护系统是真正体现微软在安全方面研发实力的新功能，它的功能主要是以下两方面：第一方面，根据特定的网络数据包特征码，判定网络入侵或者漏洞注入行为并进行相应的阻止；第二方面，对于常见的协议，检查协议通信是否符合标准。例如，虽然端口看起来是 SMTP 协议所使用的 25 端口，但是实际上使用的不是 SMTP 协议。这两方面结合在一起，加上 TMG 原有的安全访问控制功能，就可以很好地保障网络通信的合法性和安全性，从而保护整体企业的信息安全性。

6. 邮件安全传输与过滤

在 E-Mail 的保护方面，目前 TMG 可以和 Exchange 的边缘传输服务器角色、Forefront Protection for Exchange 集成在一起，实现安全的邮件传输与过滤。

7. 人性化管理与集成操作

从 ISA Server 2004 开始，ISA Server 的管理界面一直都非常友好，在 ISA 2006 中，针对部分操作又进行了简化，并提供了大量的配置向导来辅助管理操作。在 TMG 中，针对安装配置又进行了更为人性化的配置简化。当安装好 TMG 第一次进入 TMG 管理控制台时，

会自动调用开始配置向导，从而协助用户更快地完成 TMG 的配置工作。

13.1.2　TMG 的应用

Forefront TMG 是一个高级状态检测以及应用层检测防火墙，同时还包括 VPN 以及 Web 缓存，使用户能够最大化利用现有投资，提升信息安全和性能。它是微软安全战略架构 Forefront 中的新成员，替换原来的 Microsoft Internet Security and Acceleration(ISA)，成为下一代网络边缘防护产品。基于状态检测是 TMG 的一个亮点，由此 Forefront 网络边缘防护覆盖了 OSI 七层模型中的上五层，即网络层、传输层、会话层、表示层、应用层，提高了网络安全防护的严密性。

13.1.3　安装需求

安装 ForeFront TMG 的服务器计算机需满足以下要求：

(1) 硬件要求

CPU：至少 64 位 1.86 GHz 2 内核(1 CPU x 双核)处理器；

内存：至少 2GB、1 GHz RAM；

硬盘：至少 2.5GB，不含 Web 缓存及临时文件所使用的磁盘空间，缓存需要存放在 NTFS 分区上；

网络适配器：至少两块网卡，1 块接内网，1 块接外网。

(2) 软件要求

操作系统为 Windows Server 2008 x64，版本为 Standard、Enterprise 或 Datacenter 的 SP2 或 R2。

Windows 角色和功能：网络策略服务器、路由和远程访问服务、Active Directory 轻型目录服务工具、网络负载平衡工具、Windows PowerShell。

DNS 服务器：TMG 不具备转发 DNS 请求的功能，必须使用额外的 DNS 服务器，或安装 DNS 服务器角色。如果内部网络中具有域控制器，应配置使用域控制器作为 TMG 的 DNS 服务器；如果没有内部的 DNS 服务器，应配置使用 ISP(因特网服务提供商，如联通、电信等)的 DNS 服务器。

安装 TMG 之前，需要在服务器上安装 Windows Server 2008 的 以下组件和应用：

- Network Policy Server
- Routing and Remote Access Services
- Active Directory Lightweight Directory Services Tools
- Network Load Balancing Tools
- Windows PowerShell
- Microsoft .NET Framework 3.5 SP1

- Windows Web Services API
- Windows Update
- Microsoft Windows Installer 4.5

(3) 网络连接要求

在安装 TMG 服务器以前，应保证 TMG 服务器与任何一个连接到的网络均通信正常，这样便于故障排错。

(4) 域成员关系

TMG 服务器可以位于工作组环境或者域环境。无论是在安装 TMG 之前或者之后，均可以将 TMG 服务器加入域或者退出域。建议在安装 TMG 之前进行域成员关系操作。

13.2　TMG 的安装与配置

本书中采用的网络拓扑架构如图 13-1 所示。

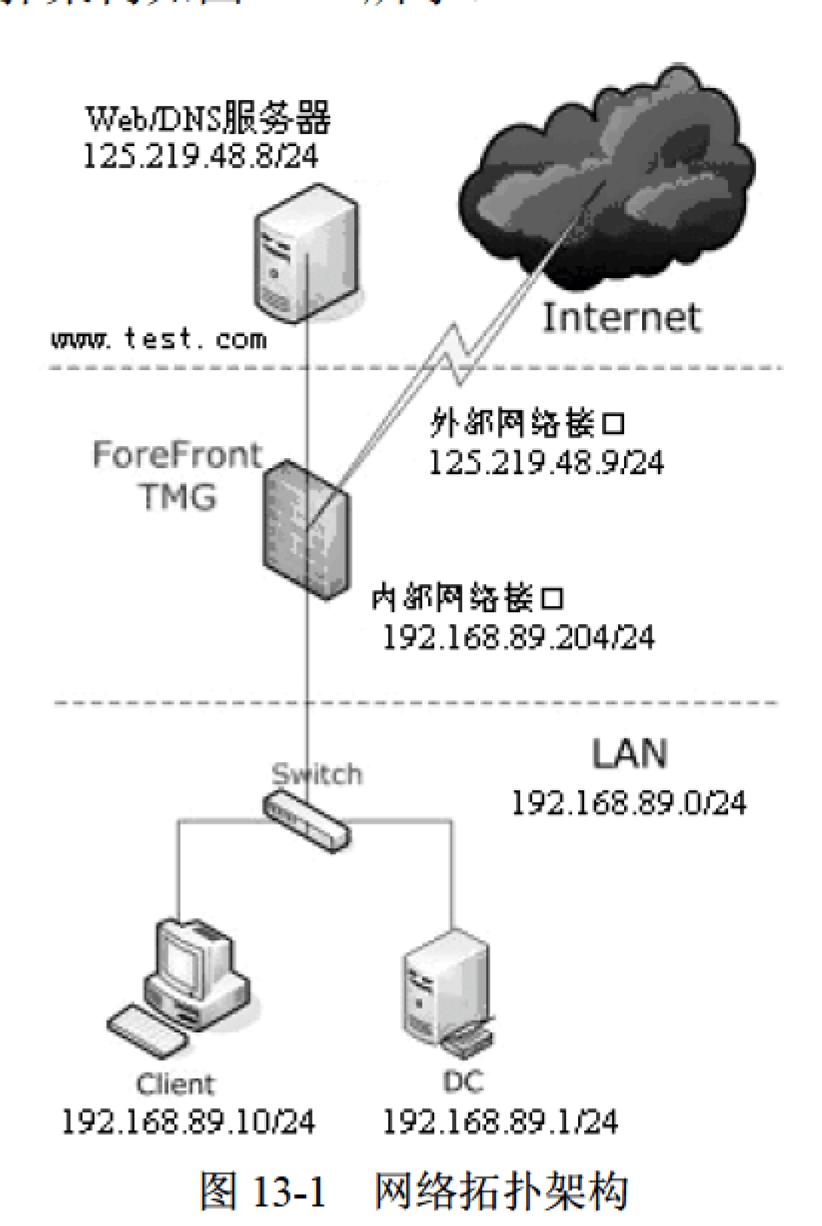


图 13-1　网络拓扑架构

ForeFront TMG 作为企业网络边缘防火墙，连接内部和外部网络。在外部网络中有一台服务器(125.219.48.8)作为 Web 服务器(http://www.test.com)和 DNS 服务器。各计算机的 TCP/IP 设置如下：

ForeFront TMG 主机的外部网络接口：

IP：125.219.48.9/24

GW：125.219.48.1

DNS：125.219.48.8

ForeFront TMG 主机的内部网络接口：

IP：192.168.89.204/24

GW：None

Web/DNS Server(专用网内部的 Web/DNS 服务器计算机)：

IP：125.219.48.8/24

GW：125.219.48.1

DNS：202.102.224.68

IIS 站点：www.test.com

Client(专用网内部的客户端计算机):

IP：192.168.89.10/24

GW：192.168.89.204

DNS：125.219.48.8

DC(专用网内部的域控制器计算机)：

IP：192.168.89.1/24

GW：192.168.89.204

DNS：125.219.48.8

参照以上参数，配置各主机和网卡。利用本书前面章节的活动目录的相关知识，建立 DC 域服务器和 Web/DNS 服务器。

13.2.1　安装 TMG

安装 TMG 的操作步骤如下：

(1) 双击 Windows Server 2008 系统光盘根目录下的 autorun.exe 程序，如图 13-2 所示，出现如图 13-3 所示的界面。

(2) 在如图 13-3 所示的界面中，单击“运行准备工具”来运行系统准备工具，从而检查安装 TMG 所需要的系统组件是否已经全部安装完成，如果没有安装，则自动进行安装。



图 13-2　运行安装程序



图 13-3　运行准备工具

(3) 在如图 13-4 所示的界面中选择安装类型，然后单击“下一步”按钮。



图 13-4　选择安装类型

(4) 在如图 13-5 所示的界面中选中“启动 ForeFront 安装向导”复选框，单击“下一步”按钮。

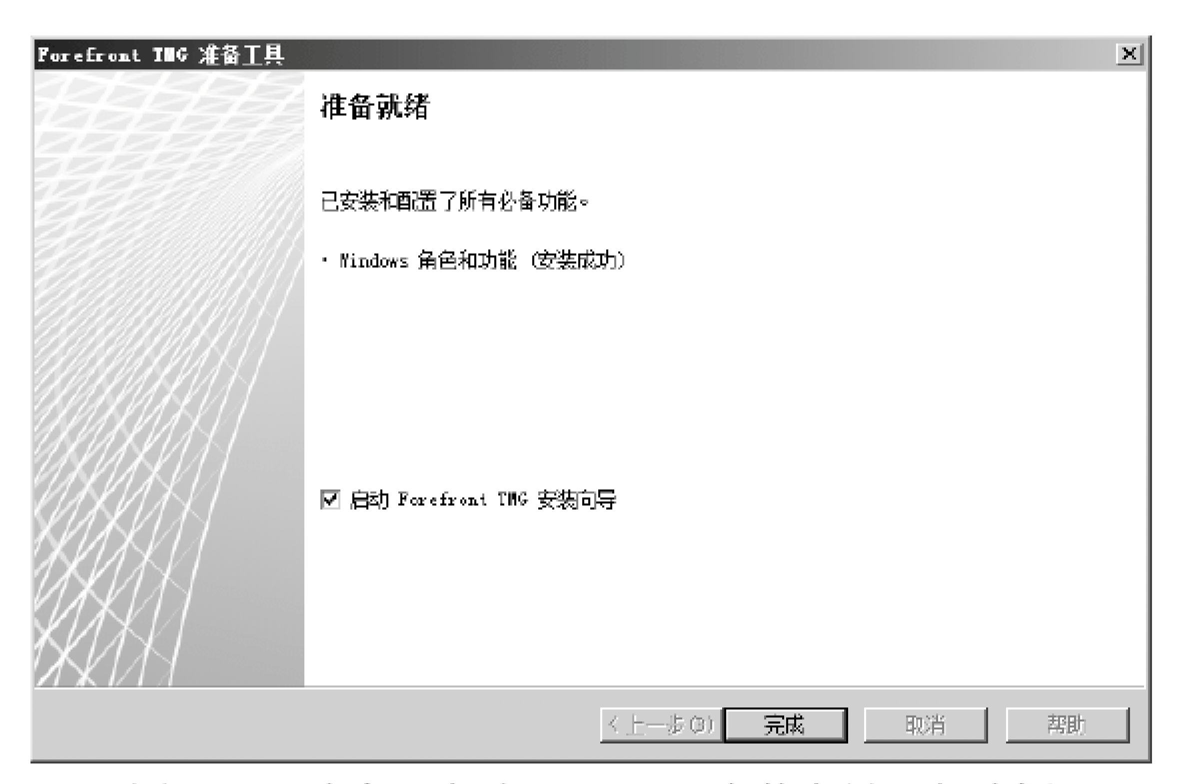


图 13-5　选中“启动 ForeFront 安装向导”复选框

(5) 在如图 13-6 所示的界面中单击“下一步”按钮。

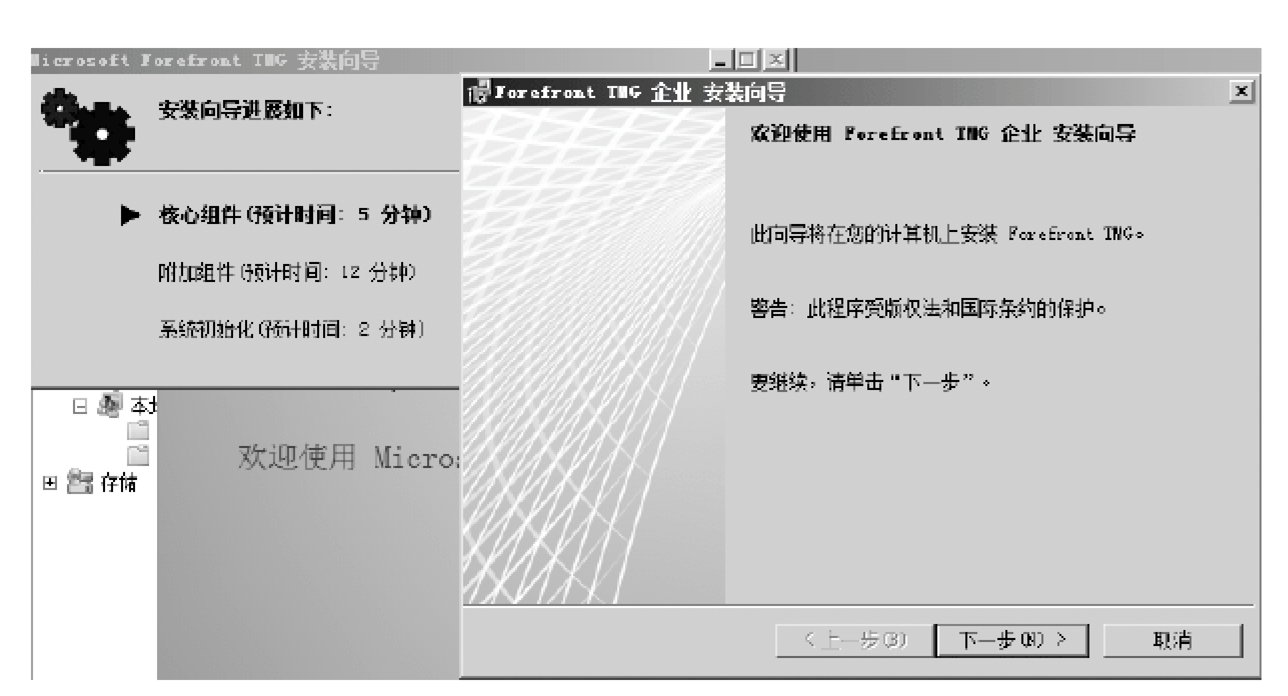


图 13-6　“ForeFront 安装向导”启动

(6) 选择接受协议许可，单击“下一步”按钮，如图 13-7 所示，输入客户信息和产品序列号，然后单击“下一步”按钮。

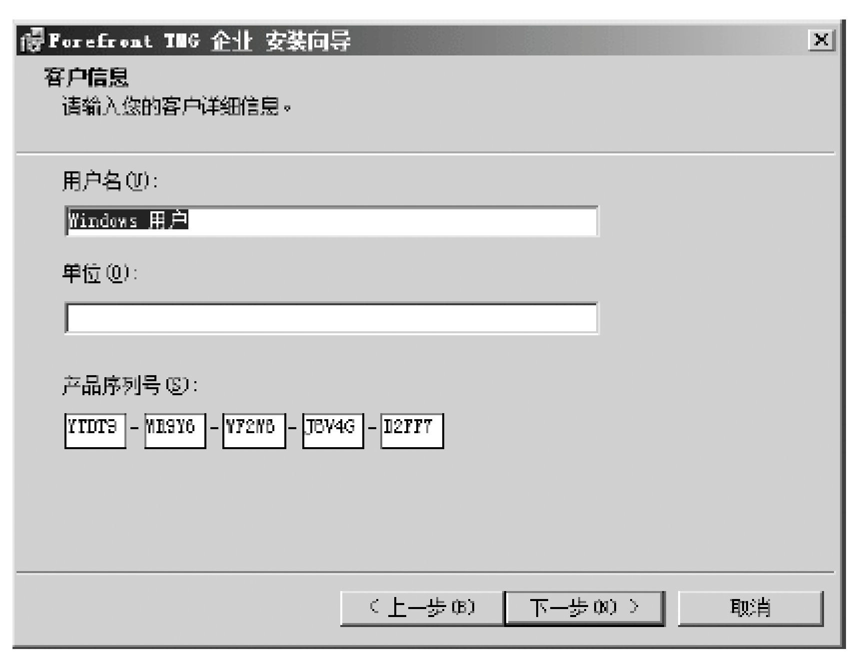


图 13-7　输入客户信息和产品序列号

(7) 在如图 13-8 所示的界面中，选择 TMG 的安装路径(TMG 只可安装在 NTFS 分区上)，然后单击“下一步”按钮，添加内网的 IP 地址范围。

可以通过网络适配器自动添加 IP 地址范围、手动添加 IP 地址范围或者添加私有 IP 地址范围。建议通过网络适配器添加 IP 地址范围。



图 13-8　选择 TMG 的安装路径

(8) 如图 13-9 所示的界面中，依次单击“添加”、“添加适配器”按钮，选中用来连

接内网的 TMG 服务器主机的网卡(如 LAN)，单击“确定”按钮。

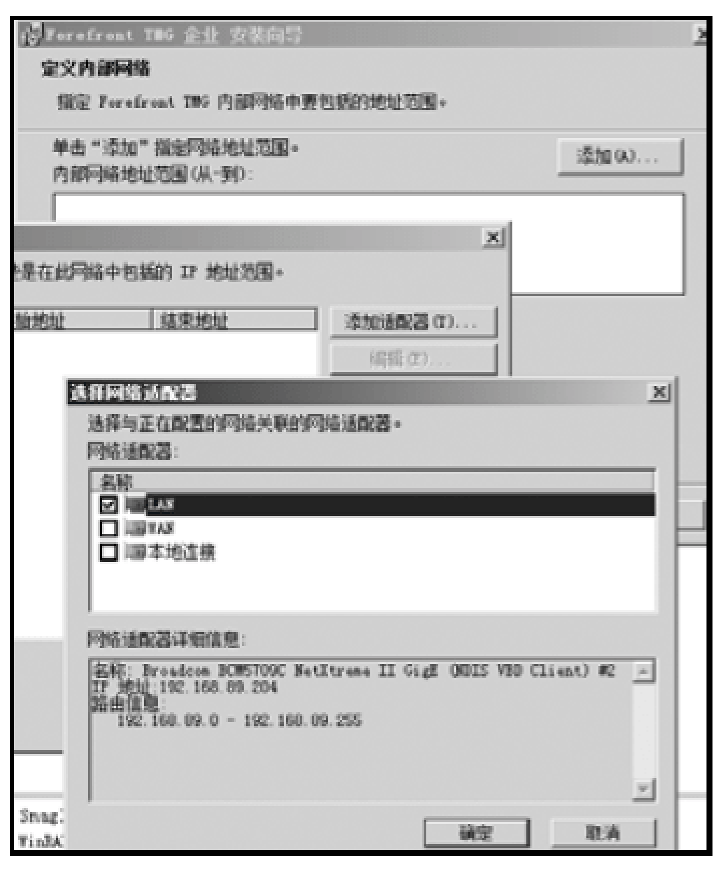


图 13-9　选择 TMG 服务器主机用来连接内网的网卡

(9) 如图 13-10 所示，输入默认的内部网络的 IP 地址范围，单击“下一步”按钮。在 TMG 中，默认的内部网络成为 TMG 进行通信的可信任网络，TMG 的系统策略会自动允许 TMG 和默认内部网络之间的部分通信。

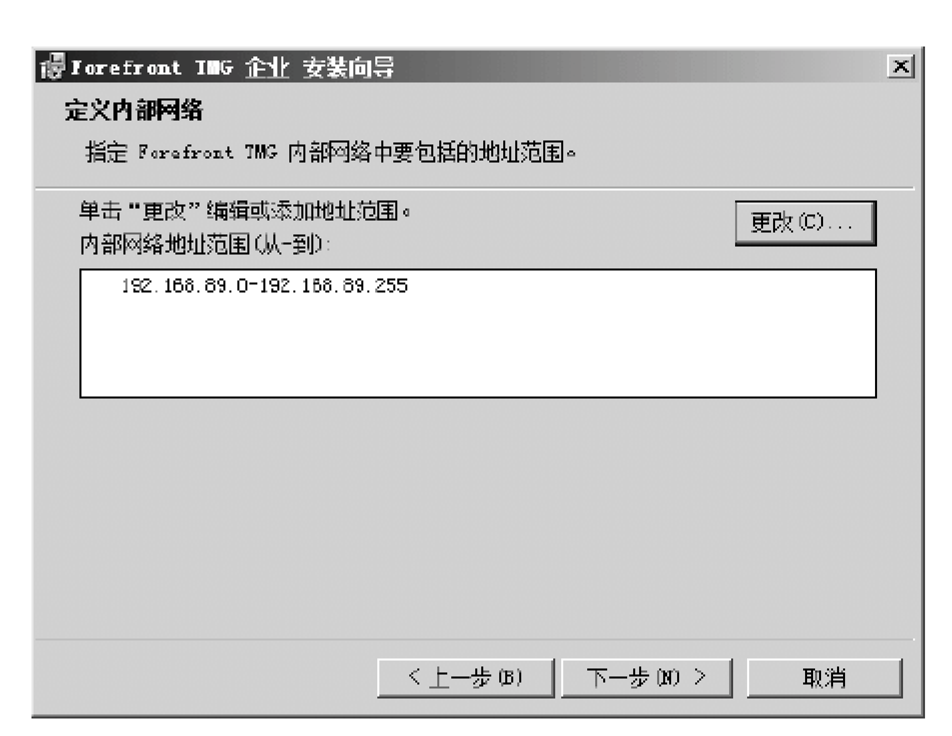


图 13-10　输入内网的 IP 范围

(10) 接着，向导提示安装的过程中有哪些服务会进行重启，如图 13-11 所示，然后依次单击“下一步”、“安装”按钮。

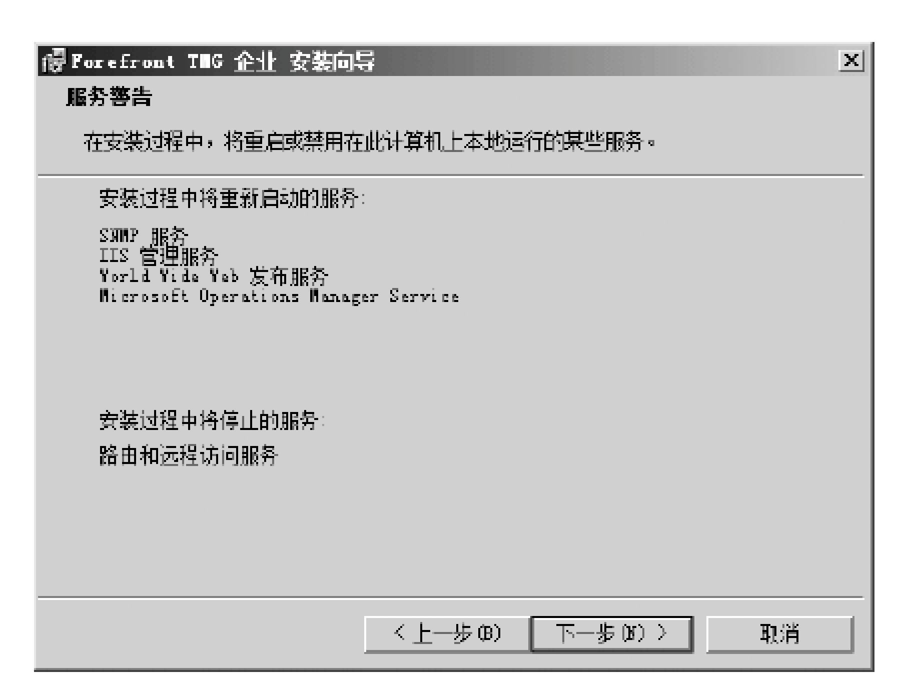


图 13-11　提示安装的过程中有哪些服务会进行重启

(11) 按照向导继续安装，安装完成后，如图 13-12 所示，单击“完成”按钮即可完成安装。

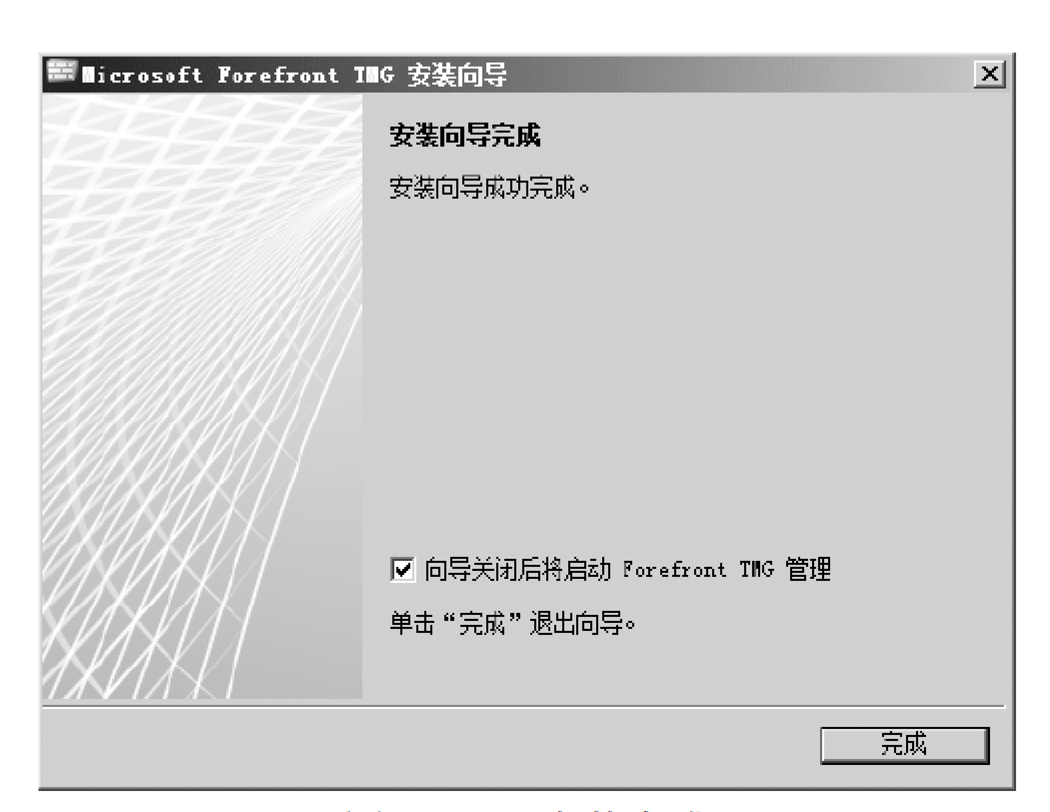


图 13-12　安装完成

13.2.2　TMG 初始化配置

Forefront TMG 的配置包括网络设置、系统设置和部署选项。网络设置的任务是为 Forefront TMG 定义关于网络配置，如 IP 地址、路由规则和网络关系。网络设置的任务是为 Forefront TMG 定义本地系统资源。配置部署选项的任务是确定 Forefront TMG 的部署和运行方式，如该 Forefront TMG 服务器以什么方式接受更新。

1. 网络设置

网络设置的配置步骤如下：

(1) 从“开始”菜单启动 Forefront TMG，进入如图 13-13 所示的设置界面，单击“配置网络设置”，在出现的“欢迎使用网络设置向导”界面，单击“下一步”按钮，出现如图 13-14 所示的“网络模板选择”界面。

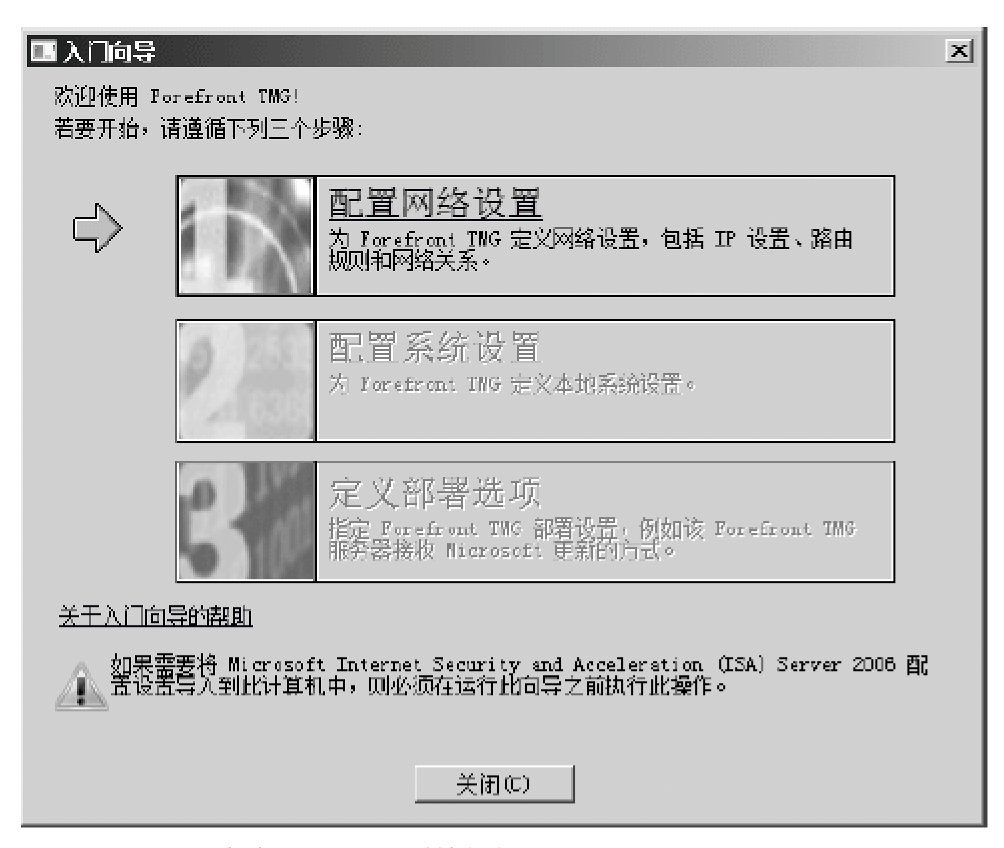


图 13-13　设置 Forefront TMG

(2) 根据应用环境选择对应的网络架构模板。在此选择“边缘防火墙”模板，如图 13-14 所示，单击“下一步”按钮。

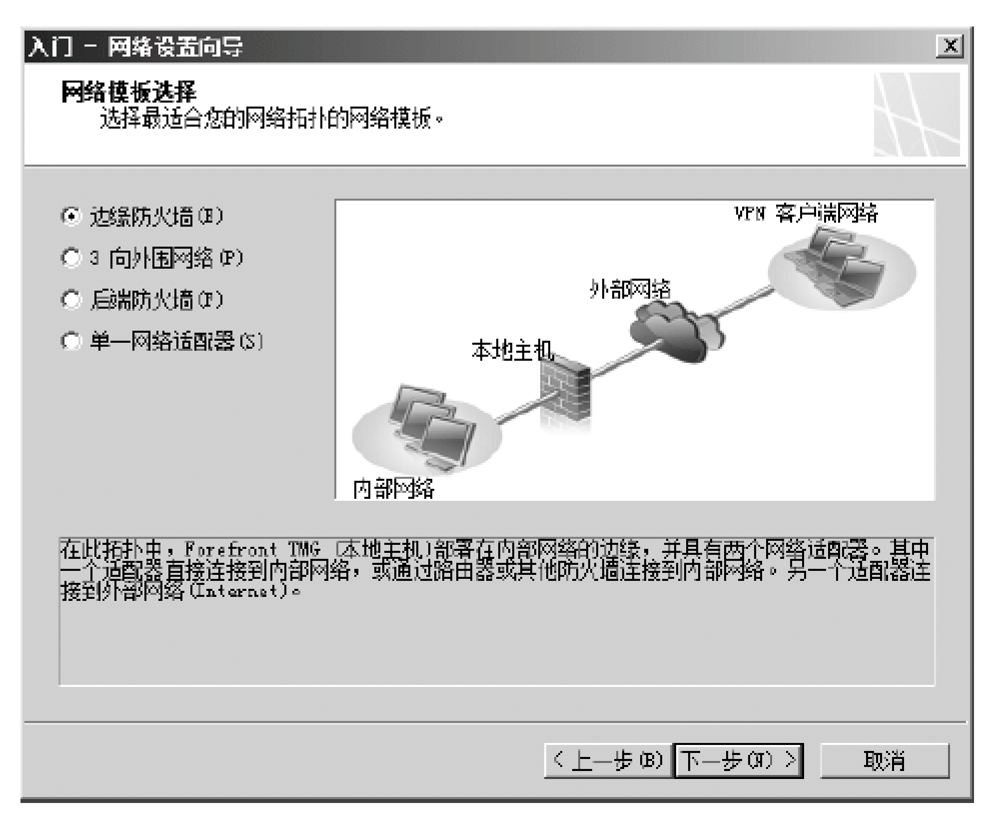


图 13-14　选择网络模板

(3) 选择到局域网的网卡(本例中该网卡的 IP 地址为 192.168.89.204)，并且可以单击“添加”按钮，添加到其他 LAN 的静态路由，单击“下一步”按钮，选择到外网如 Internet 的网卡，本例中该网卡的 IP 地址为 125.219.48.9，单击“下一步”按钮，在如图 13-15 所示的界面中单击“完成”按钮。

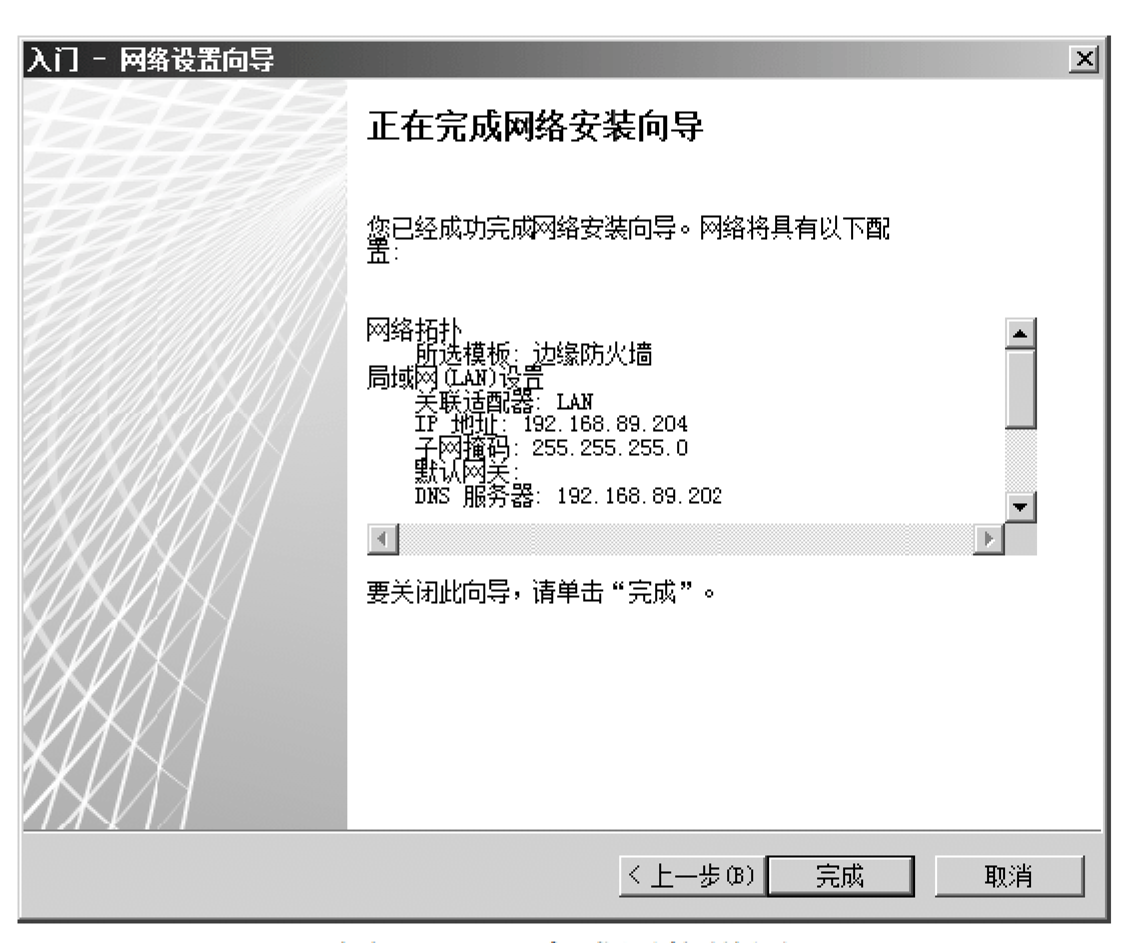


图 13-15　完成网络设置

2. 系统设置

系统设置的操作步骤如下：

(1) 在如图 13-16 所示的界面中，单击“配置系统设置”，在打开的欢迎界面中单击“下一步”按钮。

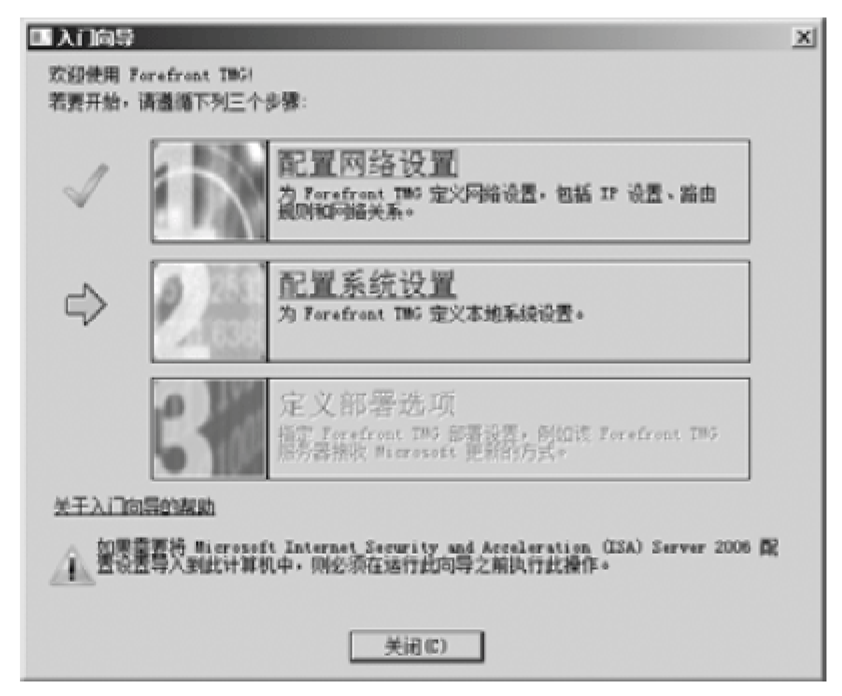


图 13-16　开始配置系统设置

(2) 在“成员”区域中选择“Windows 域”，然后单击“下一步”按钮。在出现的界面中单击“完成”按钮。

3. 部署选项

(1) 在如图 13-17 所示的界面中，单击“定义部署选项”，在打开的欢迎界面中单击“下一步”按钮。

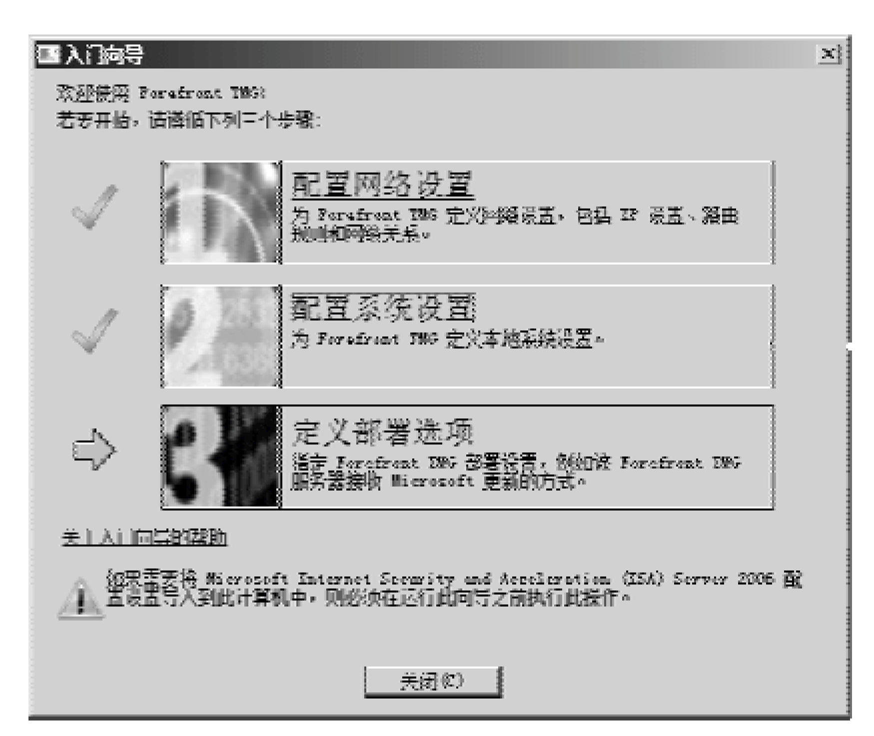


图 13-17　开始配置部署选项

(2) 在如图 13-18 所示的界面中，根据需要选择是否使用微软软件更新服务，然后单击“下一步”按钮。

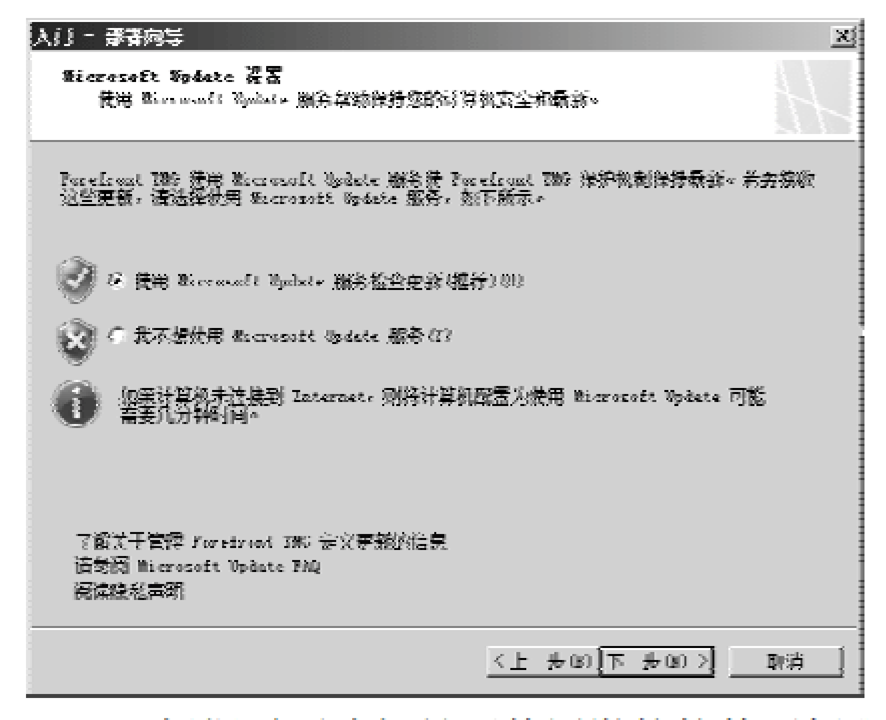


图 13-18　根据需要选择是否使用微软软件更新服务

(3) 在如图 13-19 所示的界面中，根据需要选择是否“启用恶意软件检查”，然后连续两次单击“下一步”按钮。

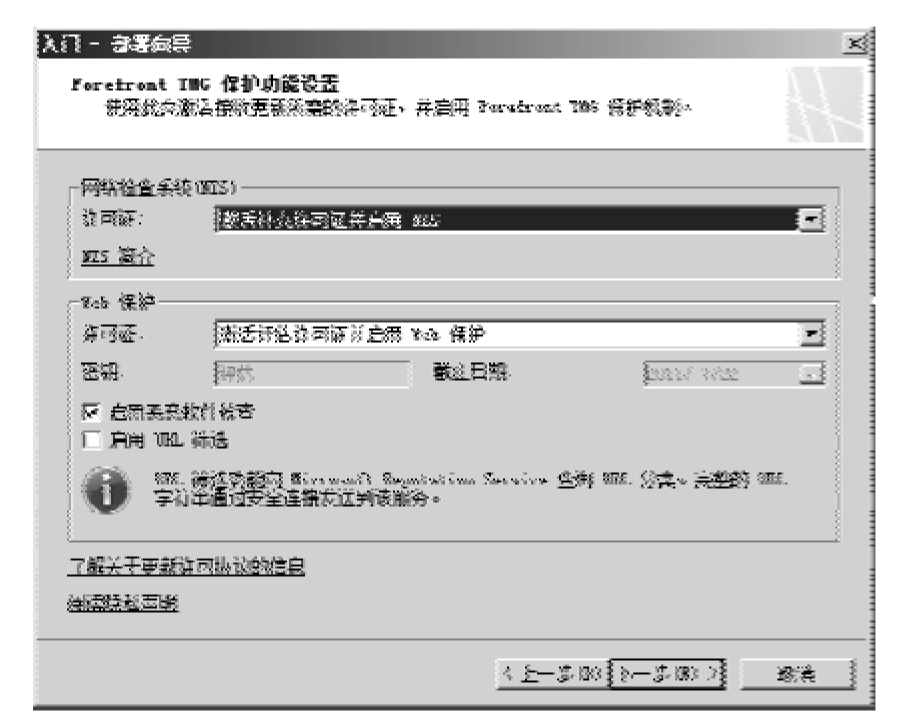


图 13-19　根据需要选择是否“启用恶意软件检查”

(4) 在如图 13-20 所示的界面中，根据需要选择微软的“客户体验改善计划”，然后单击“下一步”按钮。

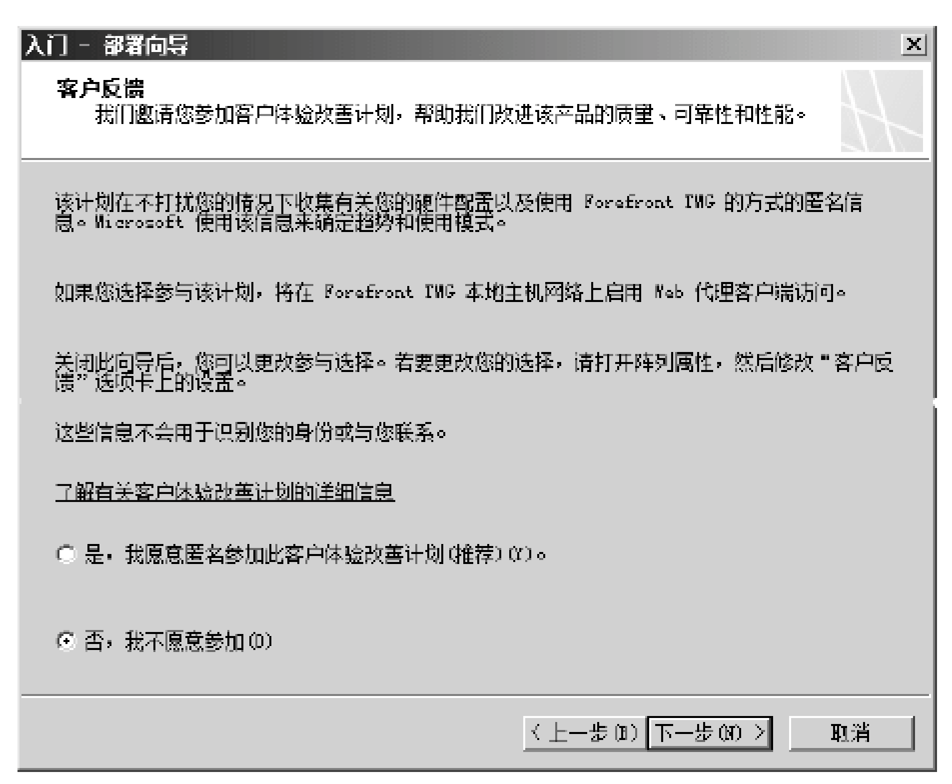


图 13-20　根据需要选择微软的“客户体验改善计划”

(5) 在如图 13-21 所示的界面中，根据需要选择是否参与或参与微软回收反馈消息的方式，然后单击“下一步”按钮。

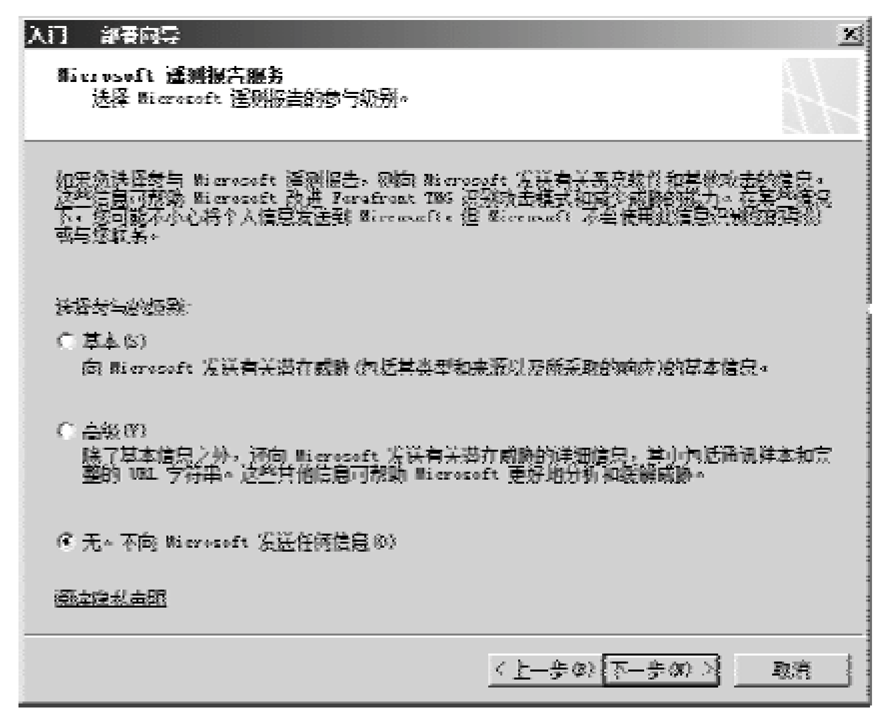


图 13-21　根据需要选择是否参与或参与微软回收反馈消息的方式

(6) 在如图 13-22 所示的界面中，单击“完成”按钮。

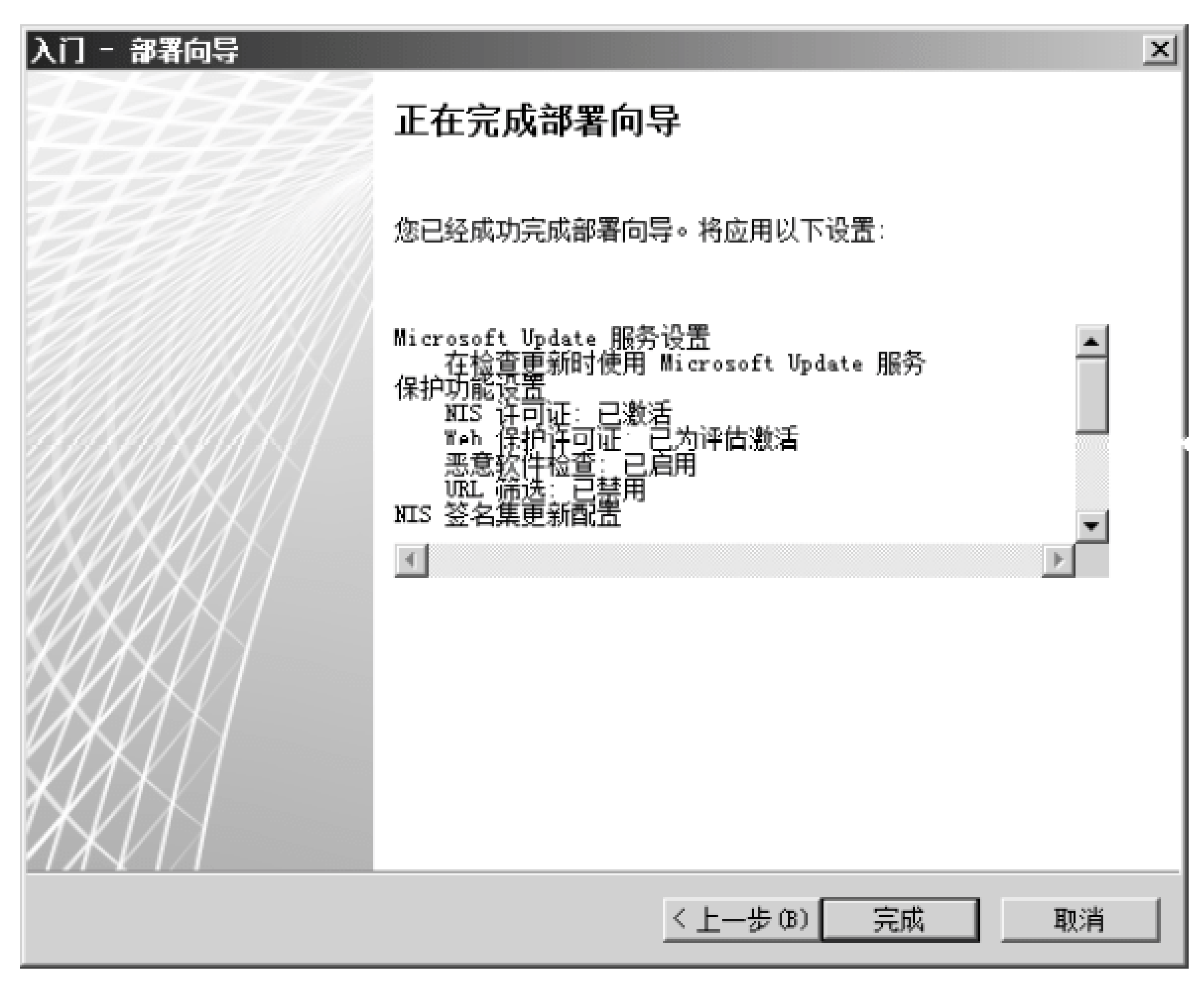


图 13-22　完成部署选项的配置

3 种配置都结束后，在如图 13-23 所示的界面中单击“关闭”按钮，打开 Web 访问策略配置向导。

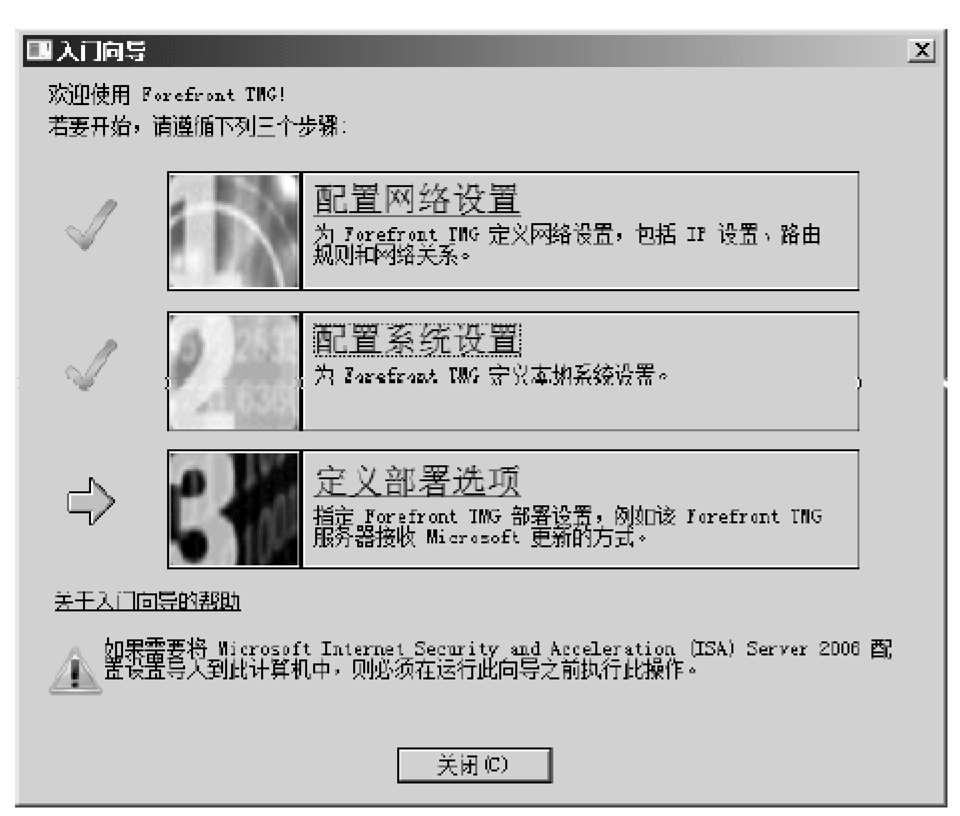


图 13-23　完成配置任务

13.2.3　创建访问策略

TMG 2010 安装好后，默认规则是阻止所有网络通信的，客户端甚至连 TMG 服务器都连接不上，所以必须建立访问策略。

1. 创建 Web 访问策略

步骤如下：

(1) 在如图 13-24 所示的界面中，单击“下一步”按钮，选中“是，创建规则来阻止

推荐的最少 URL 类别”单选按钮，如图 13-25 所示，单击“下一步”按钮。

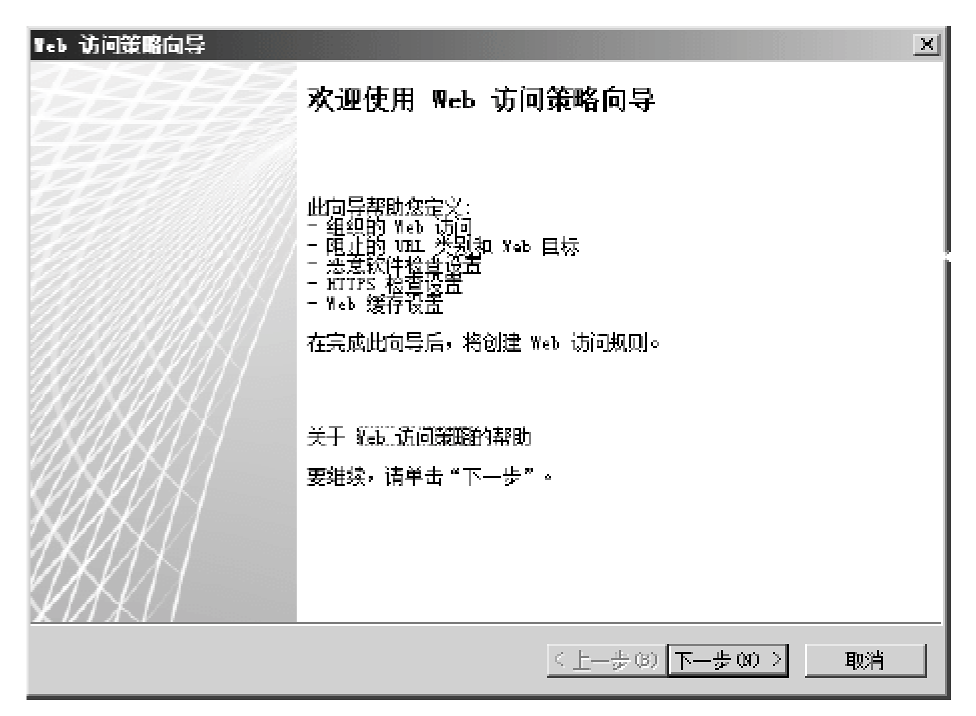


图 13-24　Web 访问策略配置向导

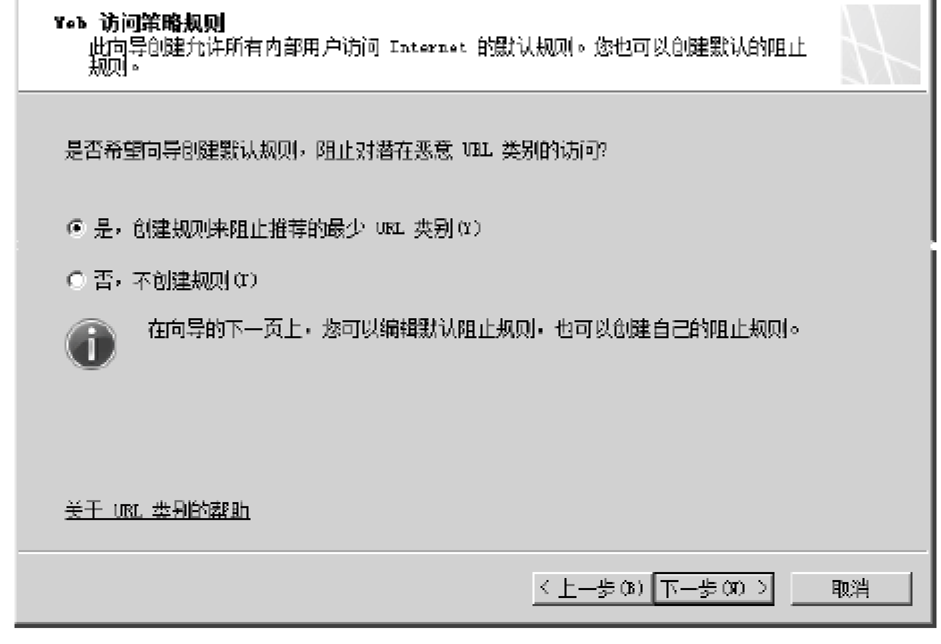


图 13-25　选择创建规则

(2) 如图 13-26 所示，配置将被策略阻止的目标 Web 网站列表，即配置黑网站名单。在 TMG 中有系统自带的一些列表，这些可以直接使用；也可以单击“添加”按钮，添加其他的关键词。出现在列表中的关键词只要存在于 Web 网站，该网站将成为策略阻止内网用户访问的对象。单击“下一步”按钮。

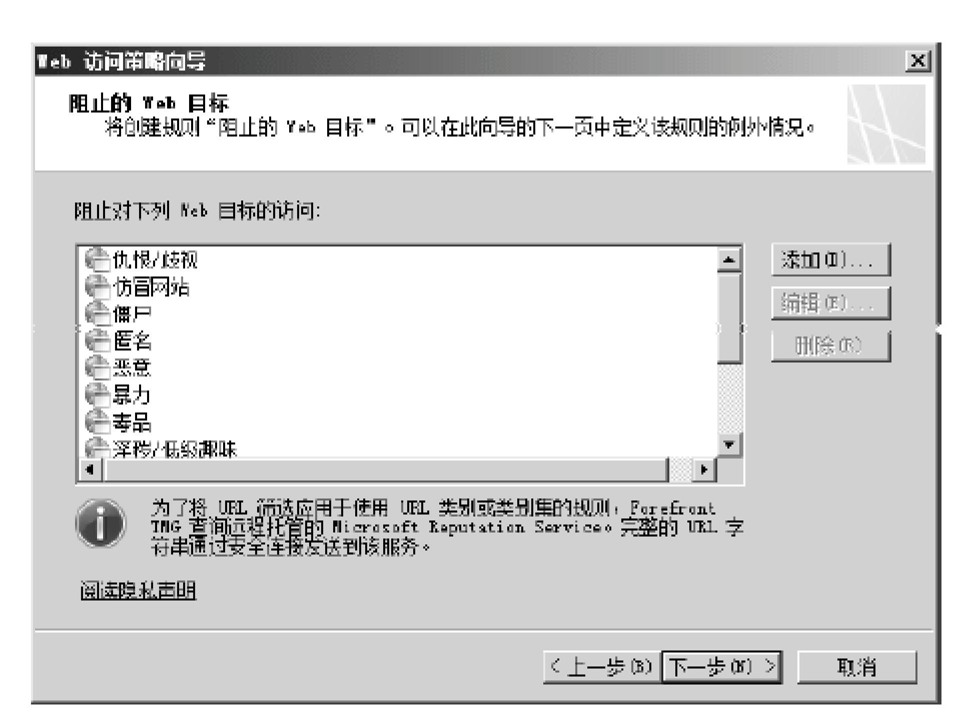


图 13-26　配置将被策略阻止的目标 Web 网站列表

(3) 如图 13-27 所示，配置不被策略阻止的内网用户列表，即配置用户白名单，单击“添加”按钮，添加有权访问外网中任何 Web 网站的用户帐号，单击“下一步”按钮。

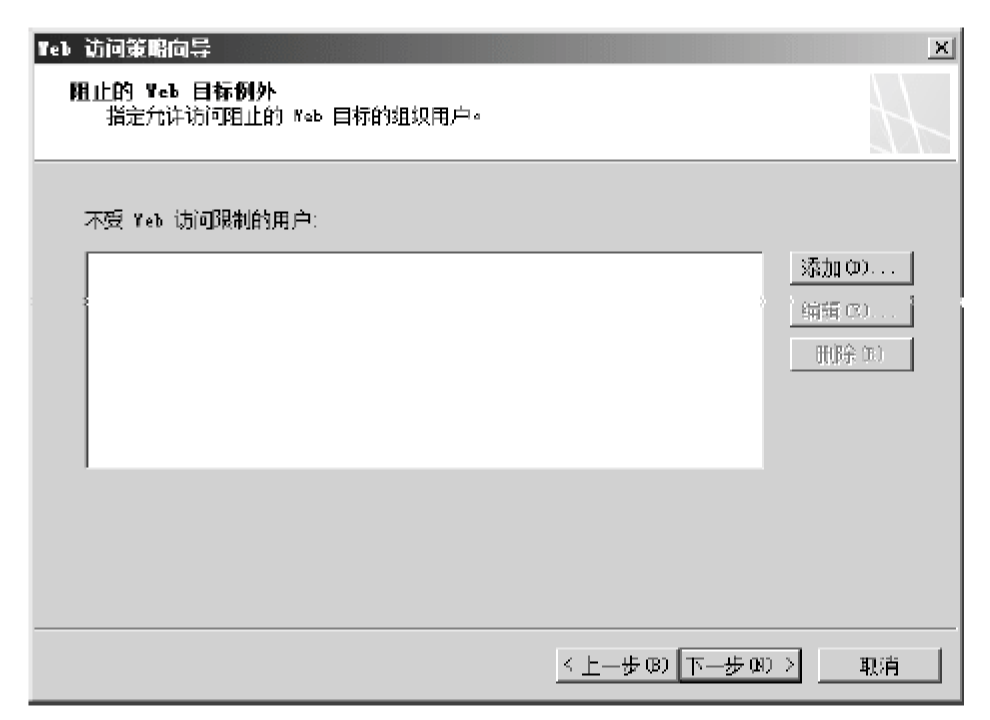


图 13-27　配置不被策略阻止的内网用户列表(即用户白名单)

(4) 如图 13-28 所示，选中“是，检查从 Internet 请求的 Web 内容”单选按钮，根据需要选择下方的复选框，单击“下一步”按钮。

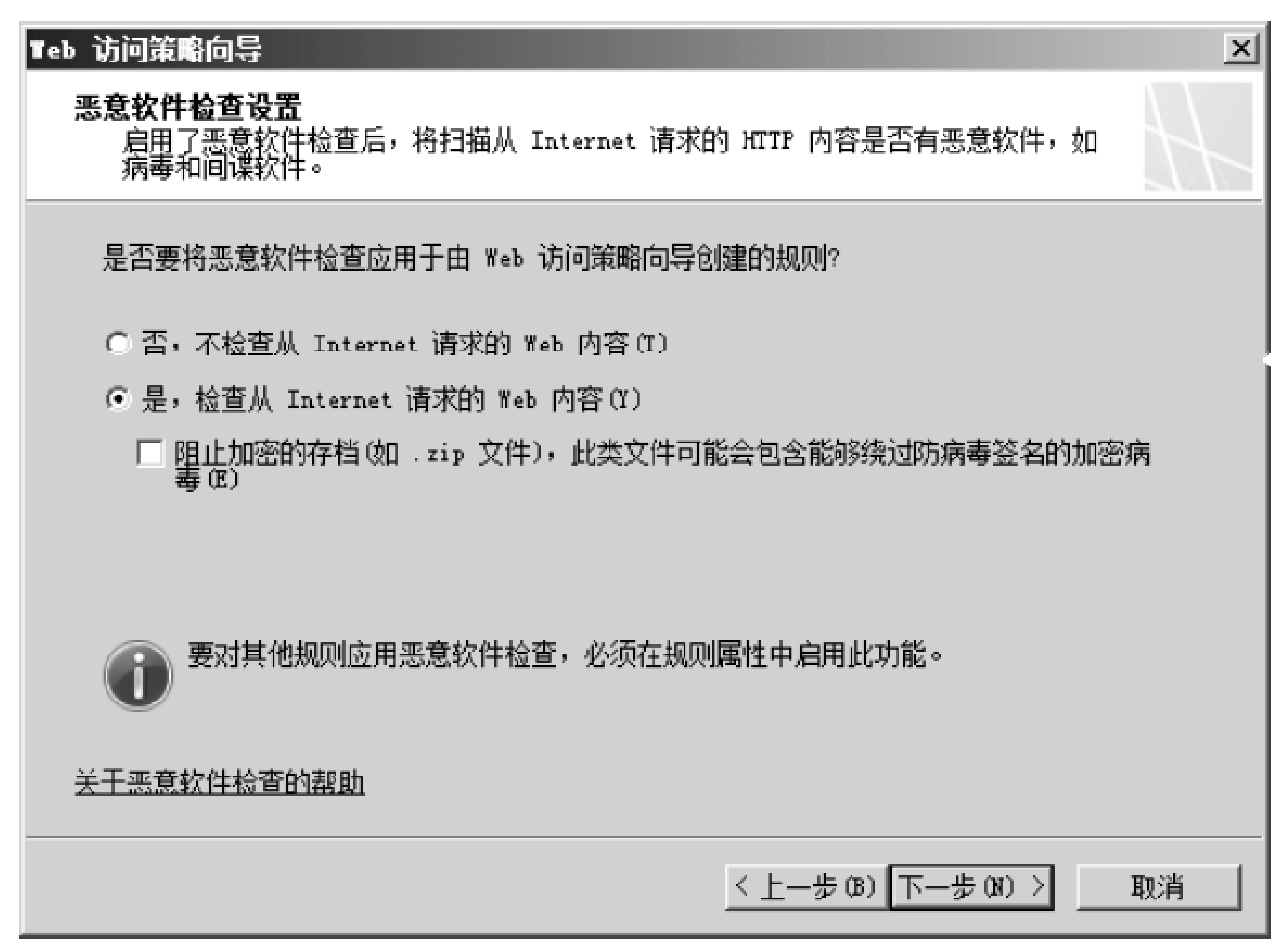


图 13-28　选择“是，检查从 Internet 请求的 Web 内容”

(5) 如图 13-29 所示，选中“允许用户与网站建立 HTTPS 连接”单选按钮，单击“下一步”按钮。

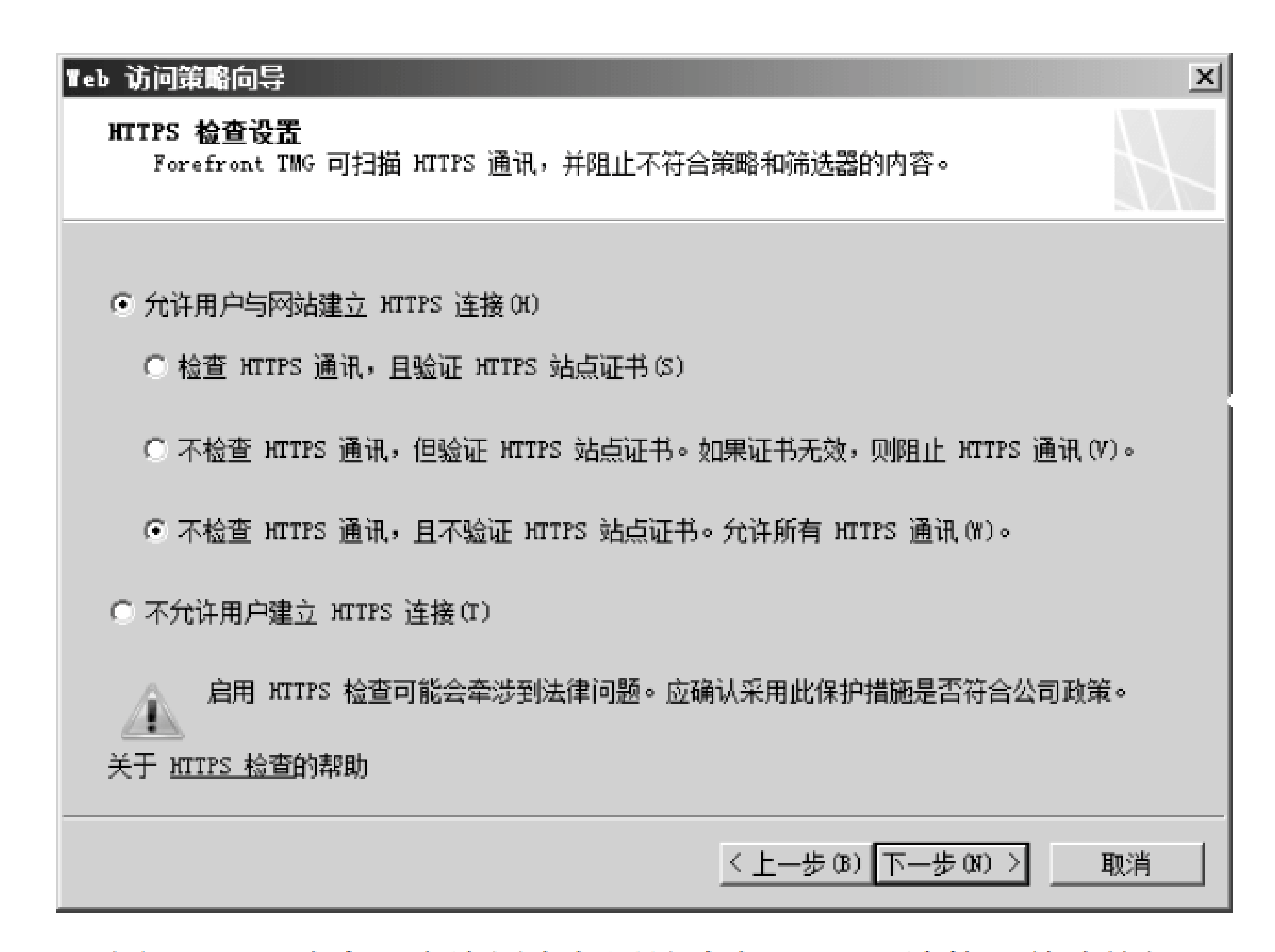


图 13-29　选中“允许用户与网站建立 HTTPS 连接”单选按钮

(6) 在如图 13-30 所示的 Web 缓存配置界面，如果想将内网用户频繁访问的网页放到缓存中以加快其访问速度，可以选中“启用默认 Web 缓存规则”复选框，单击“缓存驱动器”按钮，选择缓存空间所在的驱动器和容量，然后依次单击“确定”、“下一步”、“完成”按钮。

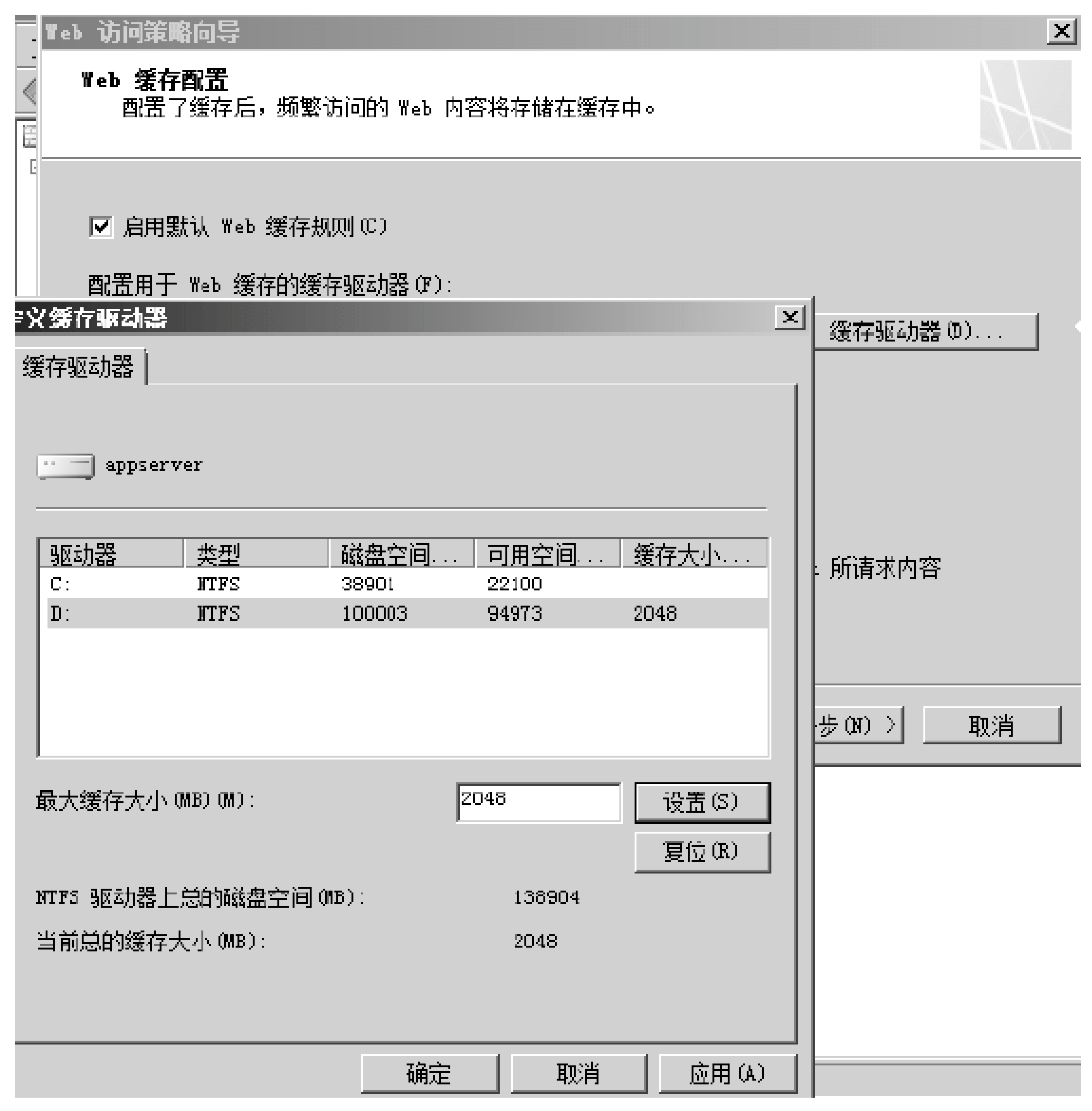


图 13-30　配置 Web 缓存

从“开始”菜单中启动 Forefront TMG，如图 13-31 所示，单击“应用”按钮使设置生效。



图 13-31　启用设置

2. 建立内网互访策略

步骤如下：

(1) 在如图 13-31 所示的界面中右击“防火墙策略”，如图 13-32 所示，在弹出的快捷菜单中选择“新建”→“访问规则”命令。



图 13-32　新建访问规则

(2) 如图 13-33 所示，输入访问规则名称，单击“下一步”按钮。

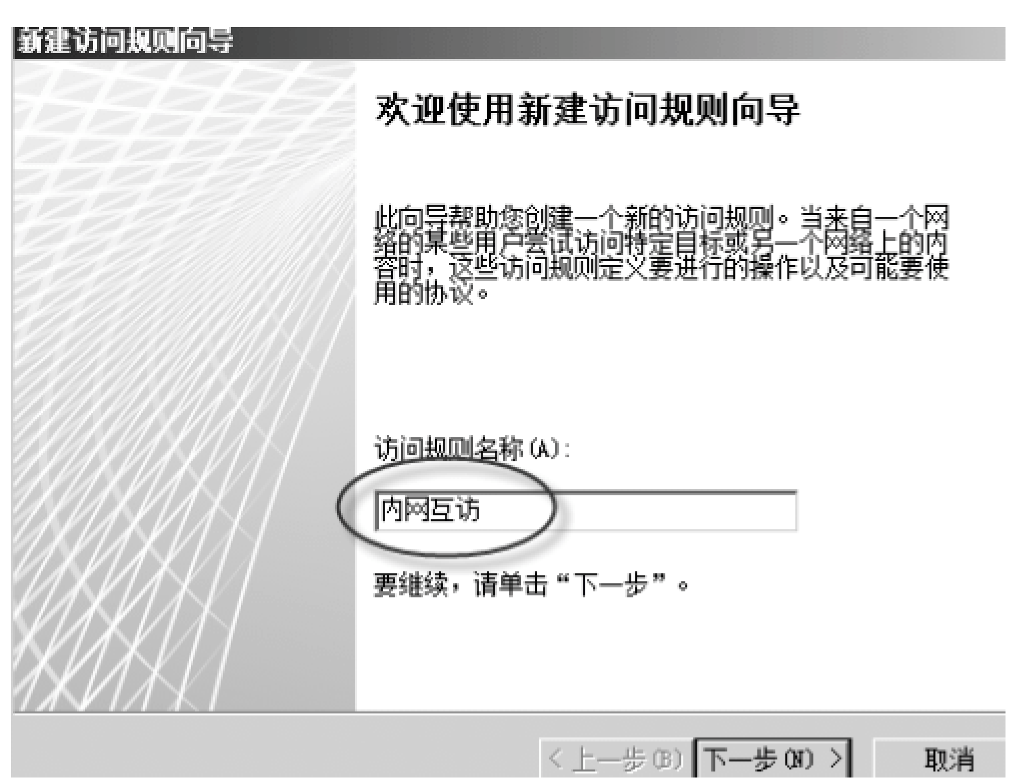


图 13-33　输入访问规则名称

(3) 如图 13-34 所示，选中“允许”单选按钮，单击“下一步”按钮。

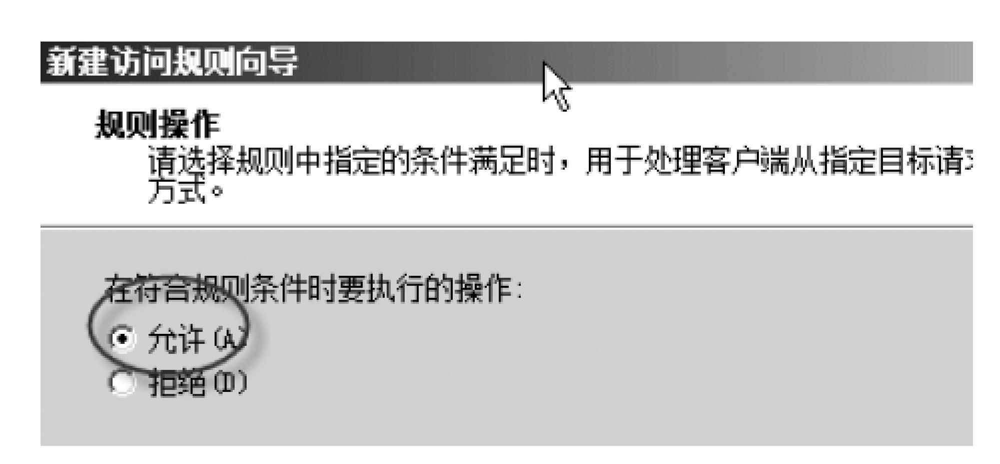


图 13-34　选中“允许”单选按钮

(4) 如图 13-35 所示，选择将此规则应用到“所有出站通讯”，然后单击“下一步”按钮。

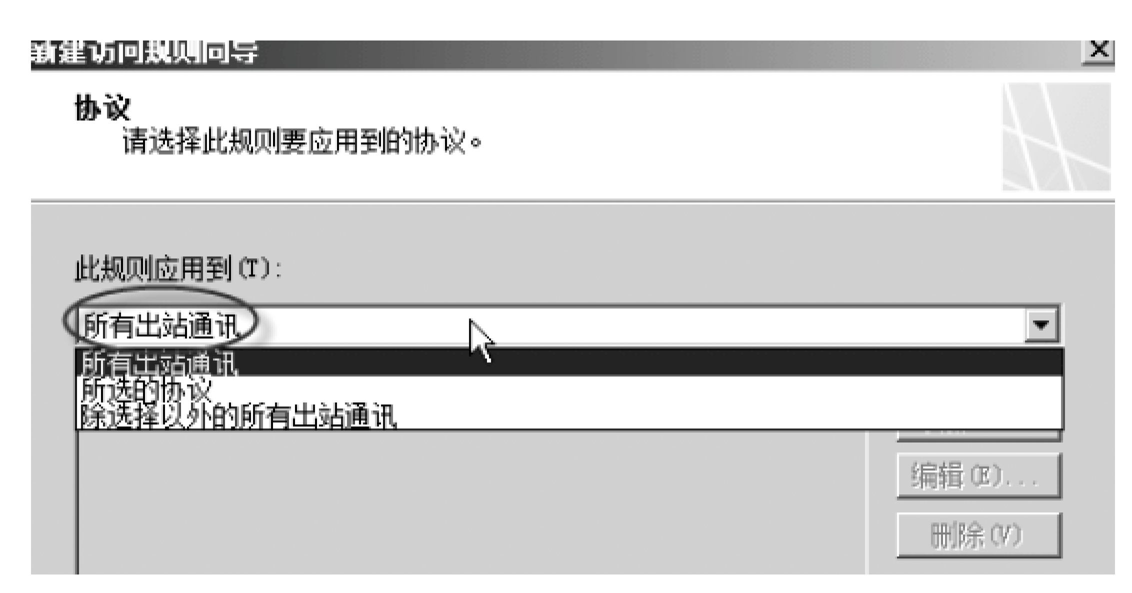


图 13-35　选择“所有出站通讯”

(5) 如图 13-36 所示，选中“对该规则启用恶意软件检查”单选按钮，然后单击“下一步”按钮。

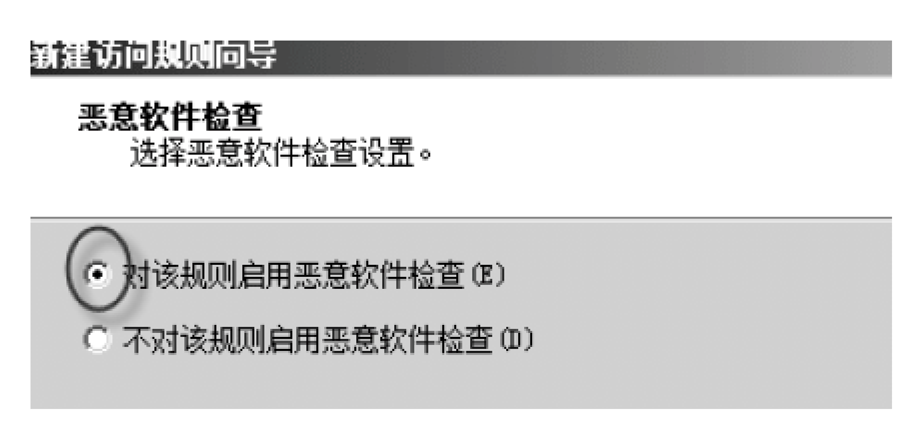


图 13-36　对新建的规则启用恶意软件检查

(6) 如图 13-37 所示，添加本地主机(即 Forefront TMG 主机)和 Forefront TMG 主机连接内网的网卡(本例中该网卡的 IP 地址为：192.168.89.204)，单击“下一步”按钮。



图 13-37　添加 Forefront TMG 主机及其连接内网的网卡

(7) 如图 13-38 所示，添加新建的规则针对的用户集，然后单击“下一步”按钮。

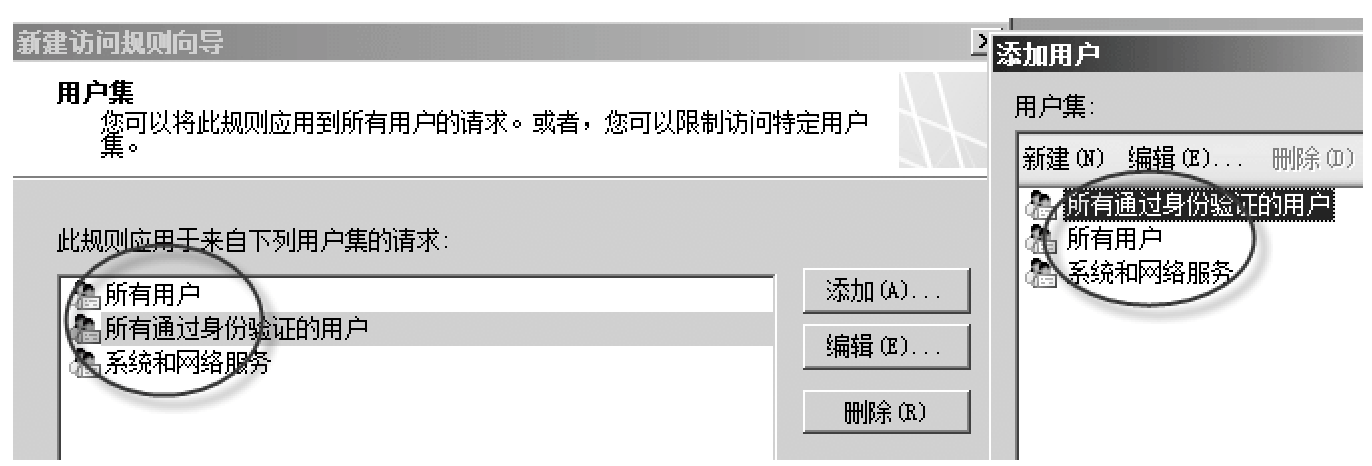


图 13-38　添加新建的规则针对的用户集

(8) 在如图 13-39 所示的界面中，单击“完成”按钮。

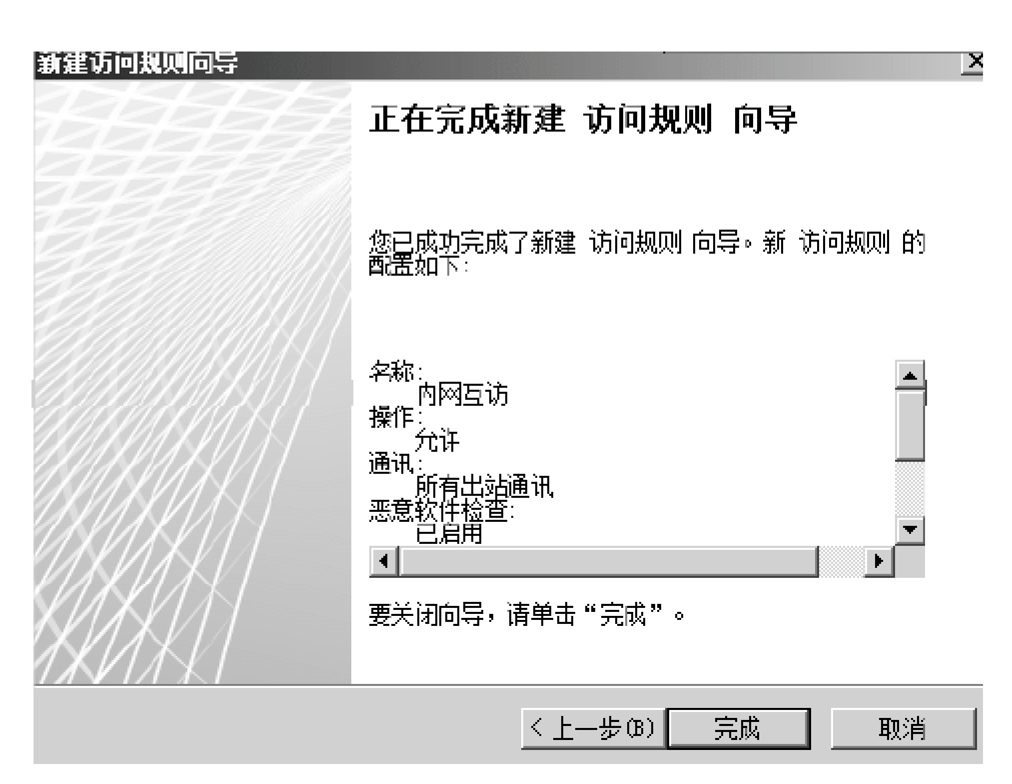


图 13-39　完成内网互访策略中相关规则的建立

如图 13-31 所示，单击“应用”按钮使设置生效。

3. 允许内网访问外网策略

步骤如下：

(1) 在如图 13-32 所示的窗口中右击“Web 访问策略”，从弹出的快捷菜单中选择“新建”→“访问规则”命令。输入访问规则名称及相关信息，如图 13-40 所示，然后切换至“操作”选项卡。

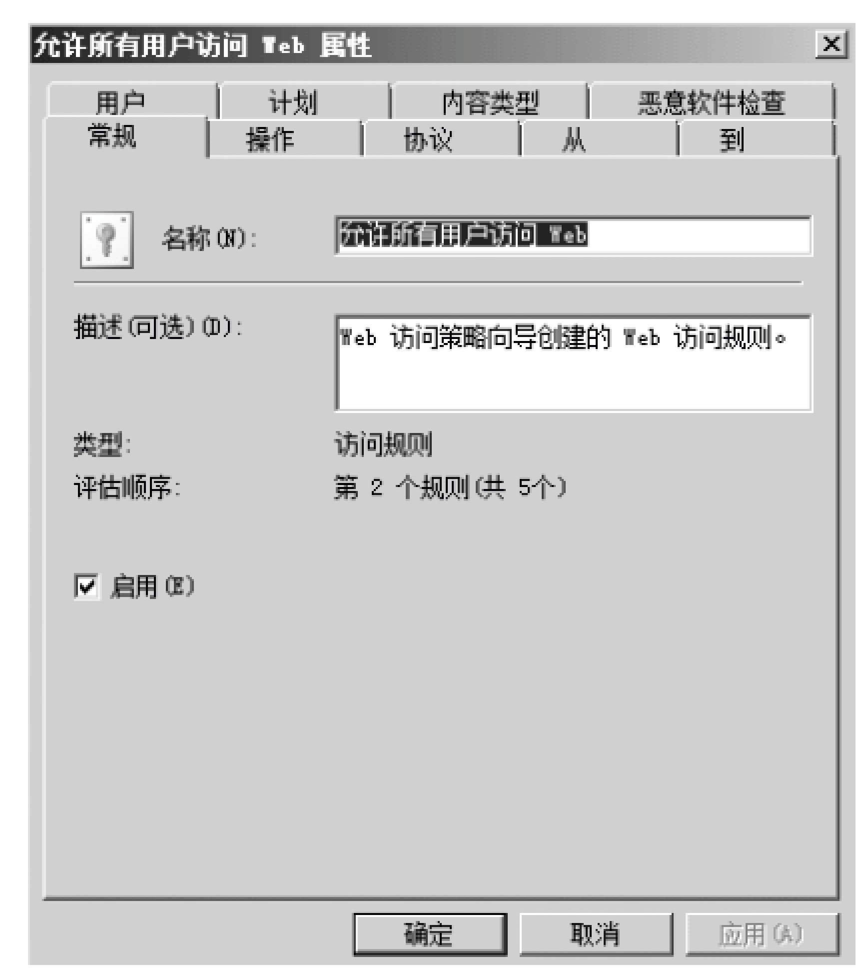


图 13-40　输入访问规则名称及相关信息

(2) 如图 13-41 所示，选中“允许”单选按钮。

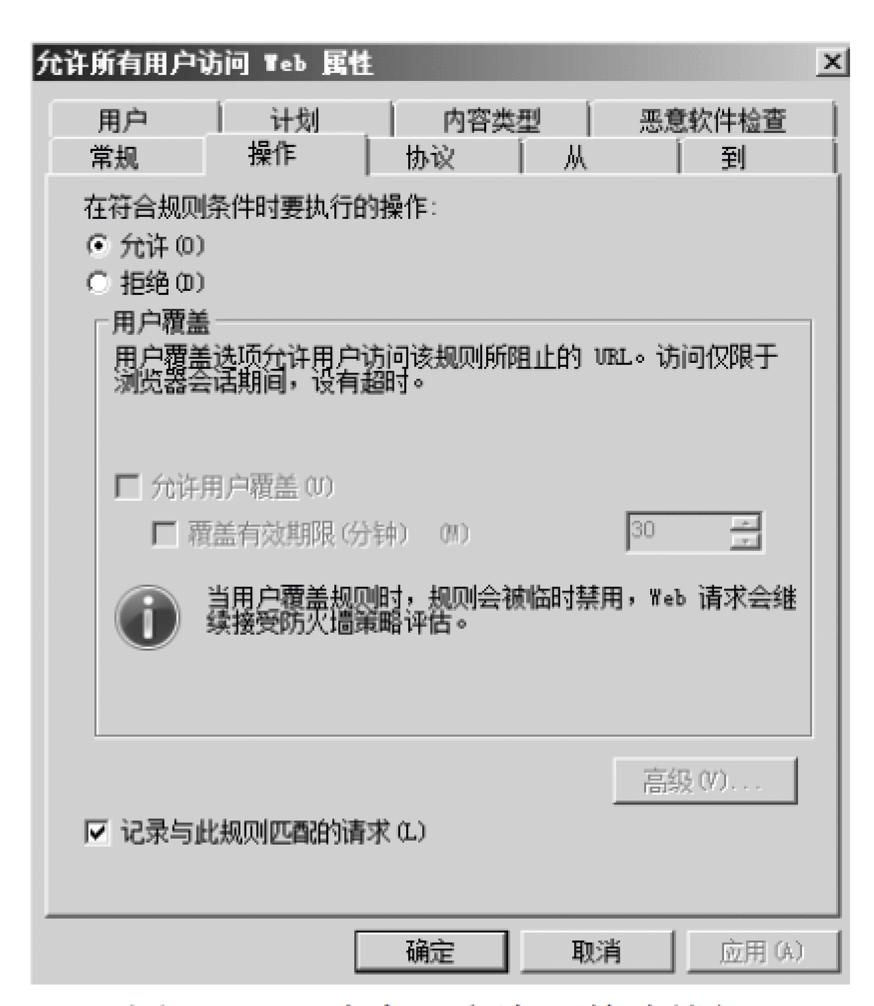


图 13-41　选中“允许”单选按钮

(3) 打开“协议”选项卡，如图 13-42 所示，在“此规则应用到”选项下，选择“所选的协议”，可以添加、删除或编辑协议列表中的网络协议。

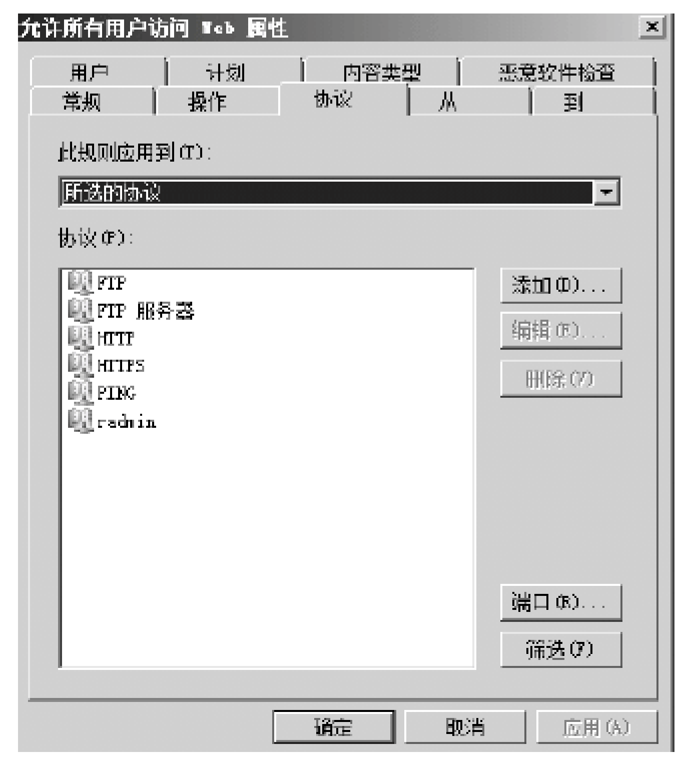


图 13-42　配置新建的规则针对的协议

(4) 打开“从”选项卡，如图 13-43 所示，添加应用了协议列表中协议的源主机，一般包括本地主机(即 Forefront TMG 主机)和 Forefront TMG 主机连接内网的网卡(本例中该网卡的 IP 地址为：192.168.89.204)。

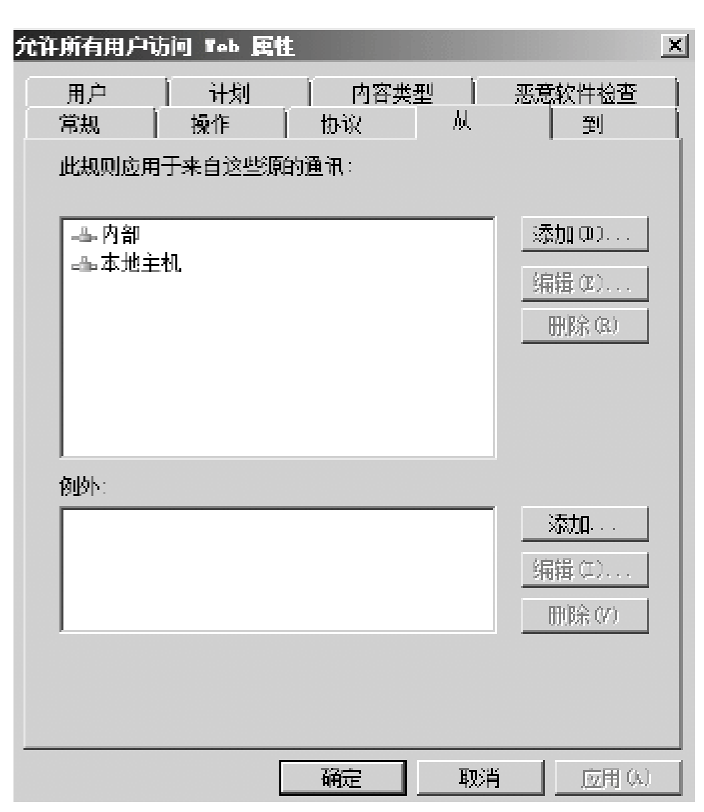


图 13-43　添加应用了协议列表中协议的源主机

(5) 打开“到”选项卡，如图 13-44 所示，添加应用了协议列表中协议的目标网站。

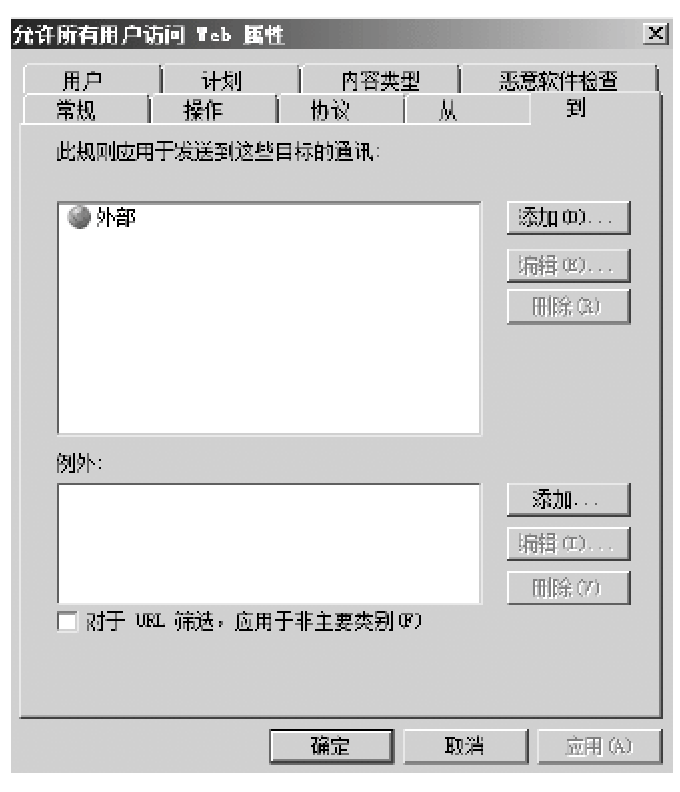


图 13-44　添加应用了协议列表中协议的目标网站

(6) 打开“恶意软件检查”选项卡，如图 13-45 所示，选中前两个复选框。

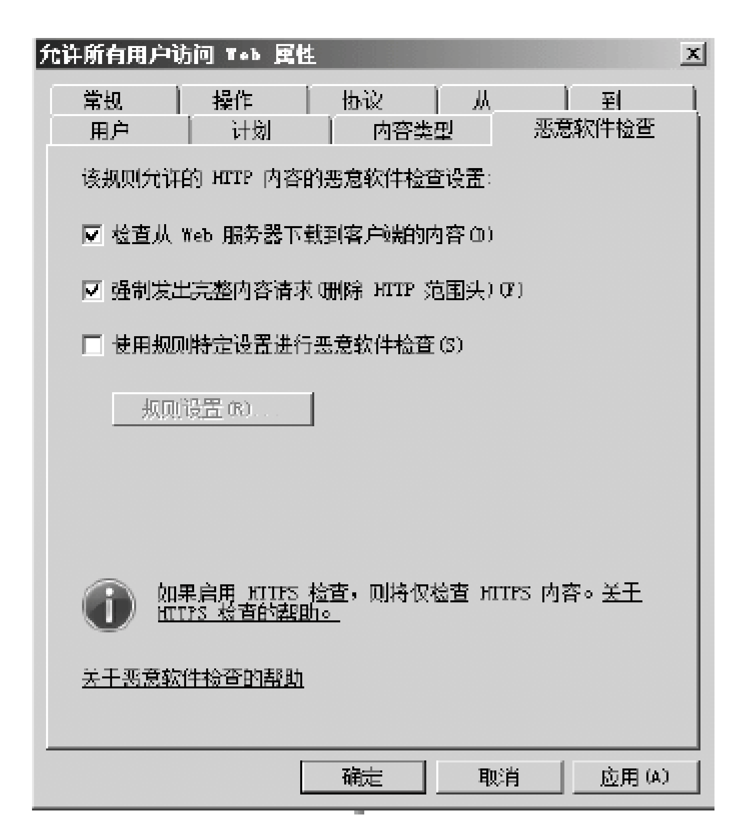


图 13-45　选中前两个复选框

(7) 打开“内容类型”选项卡，如图 13-46 所示，选择目标网站提供的部分文档类型或“所有内容类型”。

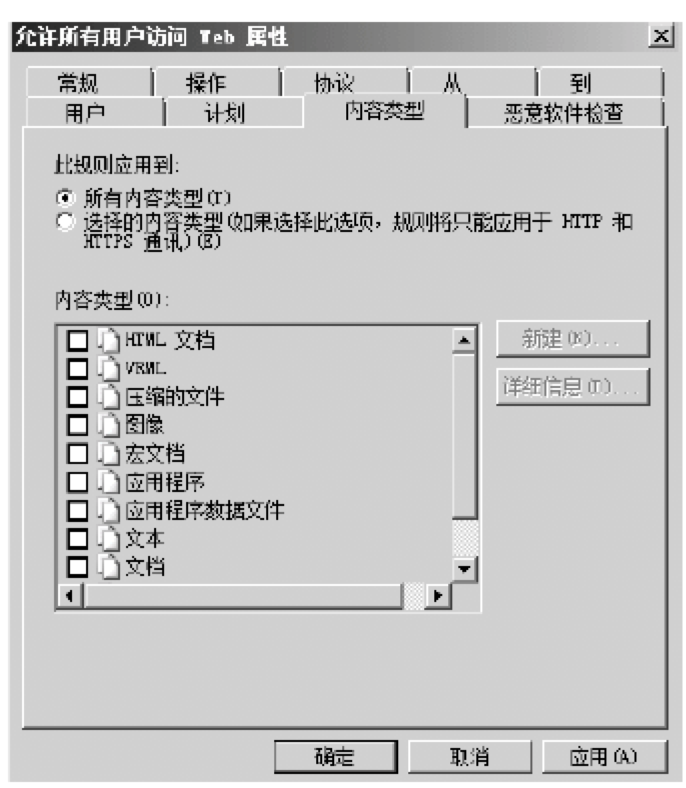


图 13-46　选择目标网站提供的部分文档类型或“所有内容类型”

(8) 打开“计划”选项卡，如图 13-47 所示，设置规则生效的时间段(即允许内网用户访问外网的时间段)或在“计划”选项右侧选择“总是”。

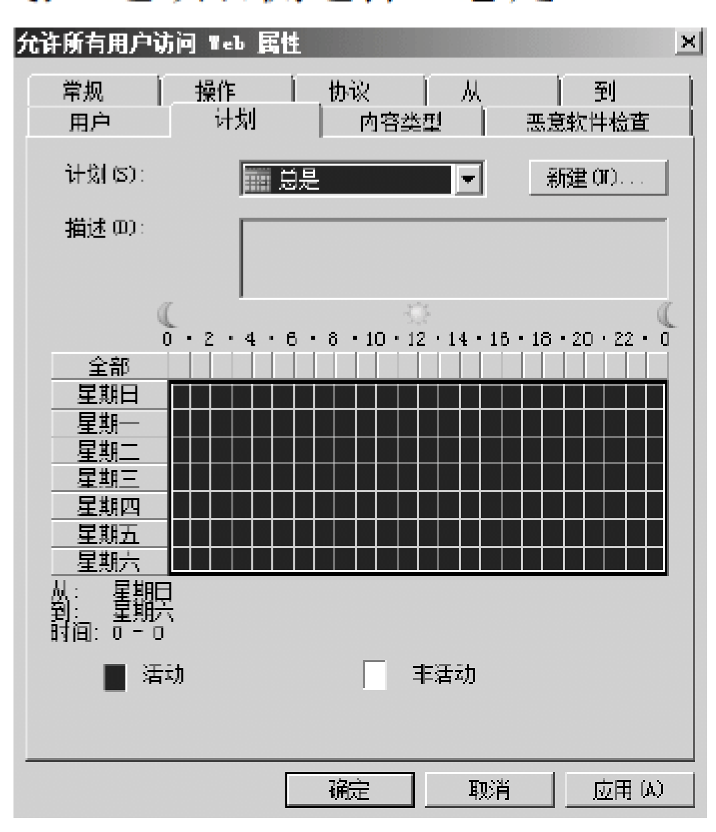


图 13-47　设置规则生效的时间段

(9) 打开“用户”选项卡，如图 13-48 所示，设置规则针对哪些用户，单击“添加”添加用户帐号，单击“确定”按钮。

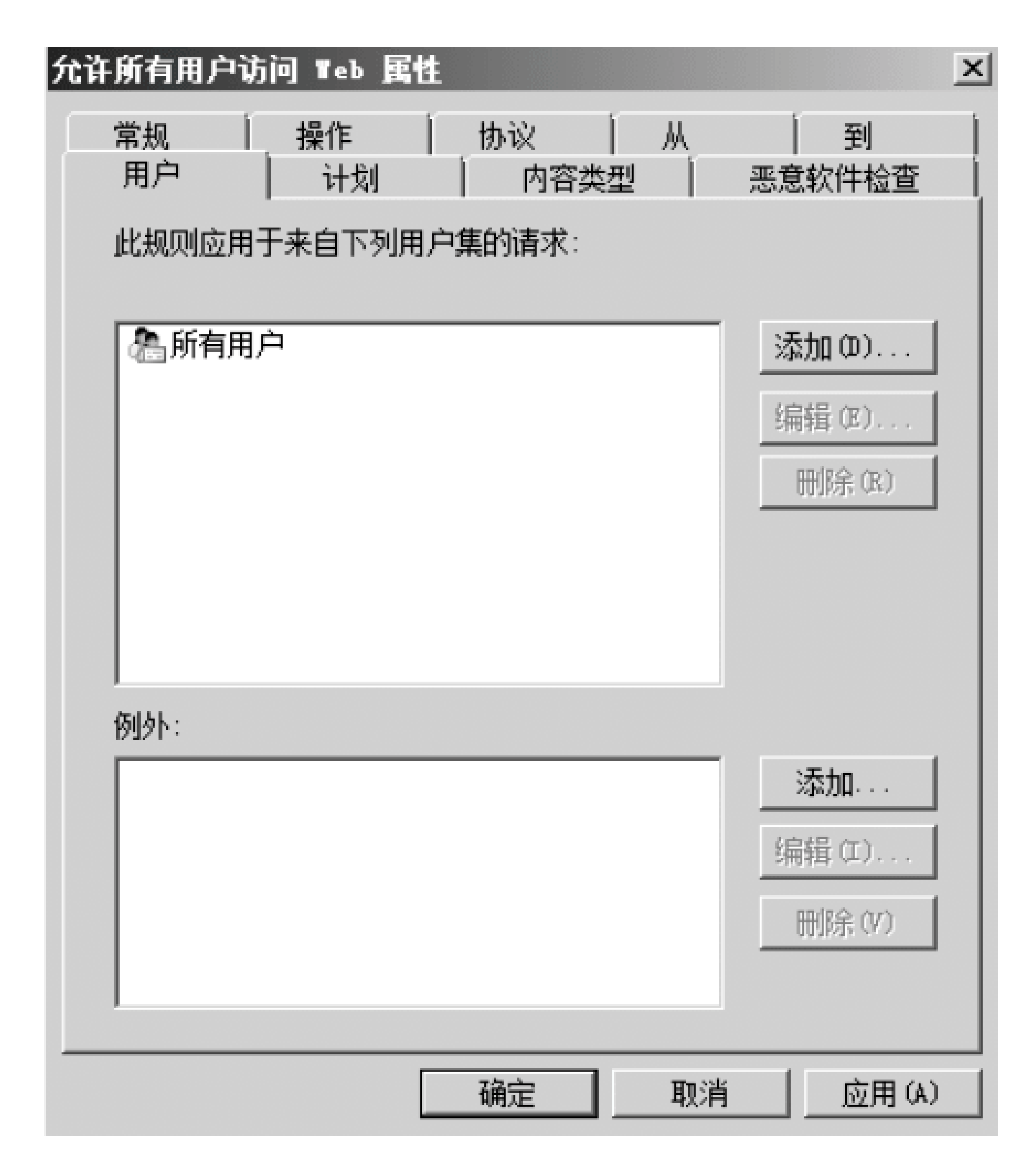


图 13-48　设置规则针对的用户集

如图 13-31 所示，单击“应用”按钮使设置生效。

4. 允许外部远程连接策略

该策略允许经过 VPN、通过外网的远程桌面或 Radmin(远程控制软件)连接到内网。除了配置访问方向相反外，其余的配置方法类似于“允许内网访问外网策略”。

如图 13-31 所示，最后单击“应用”按钮使设置生效即可。

13.3　设置客户端代理上网

如果客户端主机需要以 Forefront TMG 主机为中介访问外网，需要将 Forefront TMG 主机配置为代理服务器，简单的方法是将客户端主机的客户端软件(本书以 IE 为例)网关更改为 Forefront TMG 主机连接内网的网卡 IP 地址(192.168.89.204)。

具体步骤如下：

打开 IE 浏览器，依次选择“工具”→“Internet 选项”→“连接”，如图 13-49 所示，单击“局域网设置”按钮，选择“为 LAN 使用代理服务器”，设置代理服务器 IP(192.168.89.204)和端口号(8080)。

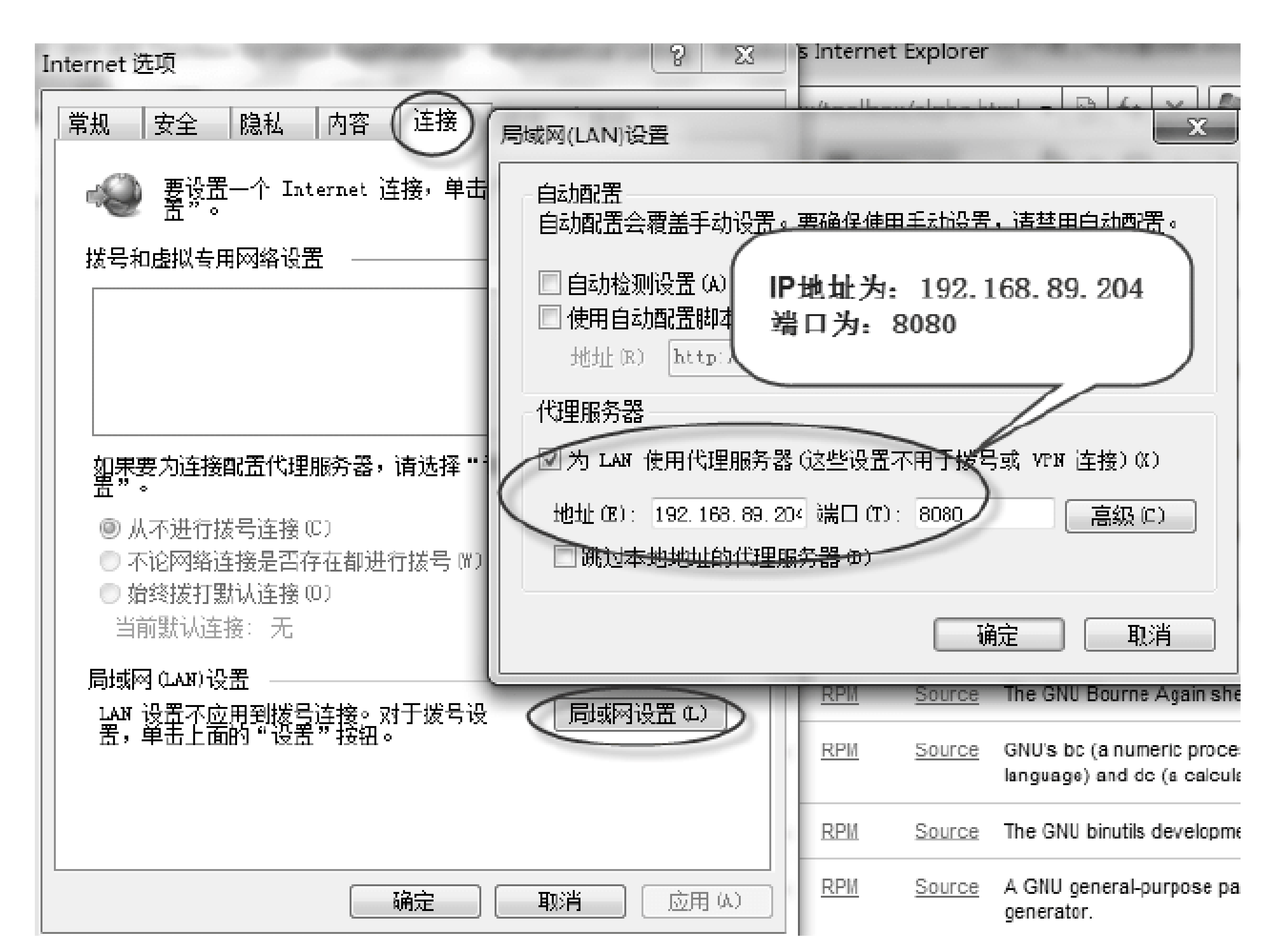


图 13-49　将 Forefront TMG 主机配置为代理服务器

此时，客户端主机上的 IE 浏览器就可以浏览外网的网页了。

13.4　本章小结

本章介绍了 Windows Server 2008 代理服务器的安装、配置和客户端的配置。代理服务器充分利用局域网出口的有限带宽，加快内网用户的访问速度，可以解决 IP 地址资源不足的问题，带动局域网很多用户上网的功能；同时代理服务器还可以作为一个防火墙，隔离内网与外网，并且能提供监控网络和记录传输信息的功能，加强了局域网的安全性，又便于对上网用户进行管理。

13.5　思考与练习

【思考题】

1. 什么是代理服务器？
2. Windows Server 2008 代理服务器的配置步骤有哪些？

【练习题】

配置 Windows Server 2008 代理服务器(参考 13.2 节)。

第14章　系统安全防护

【本章导读】

Windows Server 2008 是目前微软公司最安全的操作系统，但是任何操作系统都不可能是完美无缺的，同时黑客技术也在不断进步，这就使得系统在使用过程中受到攻击的可能性越来越大；另外，微软公司为保证系统的易用性，将部分安全功能设置为关闭或者没有安装某些功能，因此需要管理员根据自己所处的网络环境做出相应的设置。

14.1　系统更新配置

任何一个操作系统面市后，随着时间的推移，会有越来越多的缺陷和漏洞被发现，如果管理员不能及时修复这些漏洞，系统就会增加被攻击的可能，影响系统的安全性。操作系统比较危险的漏洞有以下 3 种：

- 0day 漏洞。这种漏洞由个人或某些计算机安全组织发现，目前没有对外公布，微软公司也没有提供针对该漏洞的解决方案，最容易导致操作系统被攻击。
- 1day 漏洞。这种漏洞一般由微软官方公布，并提供了解决方案，但在公布当天许多管理员还没有获得更新消息，攻击者仍能利用这种漏洞进行攻击。
- 陈旧漏洞。这种情况一般是由于系统管理员疏于管理，在较长时间内没有为操作系统安装系统更新补丁，导致系统容易被攻击。

微软公司为了提高操作系统的安全性，在发现漏洞后可以在最短时间内提供解决方案，即安全更新程序，也称为安全补丁，管理员从微软官方网站下载或通过系统更新程序下载后安装即可。

分析上面的 3 种漏洞，0day 漏洞危害最大，根本不能防范，但 0day 漏洞往往由少数人发现并掌握，而且一旦采用这种漏洞进行攻击，会很快被微软公司获取相关信息，并为管理员提供安全更新程序以修复该漏洞，因此就算 0day 漏洞危害性最大，但是危害面一般不会很大。1day 漏洞是最常被攻击者利用，危害也较大，但此时微软公司已经提供了安全更新程序，因此 1day 漏洞危害时间都比较短。第三种情况对疏于管理的服务器危害最大，却是最容易避免的。

根据以上分析，管理员可以及时安装微软公司发布的安全更新程序来将漏洞带来的危害降到最低。

14.1.1　手动更新的配置

管理员可根据需要随时查看微软公司是否发布新的安全更新程序，具体操作方法如下：

(1) 依次选择“开始”→“控制面板”命令，打开控制面板，双击 Windows Update 图标，打开 Windows Update 界面，如图 14-1 所示。



图 14-1　Windows Update 界面

(2) 单击“检查更新”按钮，如果此时服务器和 Internet 相连接，即可连接到微软官方网站查找安全更新程序，如图 14-2 所示。



图 14-2　Windows Update 检查更新界面

(3) 如果有可用更新，根据提示进行下载更新即可，如图 14-3 所示。



图 14-3　Windows Update 安装更新界面

如果要进行手动跟新，单击“安装更新”按钮即可。

14.1.2　安全补丁的自动更新

上述方法只能实现手动更新，自动化程度不高。可以说，系统的安全性直接取决于管理员更新系统的频率，这样就大大增加了安全隐患。Windows Server 2008 还提供了自动更新，设置方法如下：

(1) 打开 Windows Update 界面，单击左侧的“更改设置”，打开自动更新配置界面，默认设置为“自动安装更新(推荐)”，管理员可在下面“安装新的更新”中设置检查并安装安全更新程序的频率和时间。此时系统将按照设置好的频率和时间下载更新程序并自动安装，也可以展开下拉菜单，选择其他选项，如图 14-4 所示。



图 14-4　Windows Update 更新设置界面

(2) 菜单中各选项的含义分别如下。

- “下载更新，但让我选择是否安装更新”：仅下载更新程序，然后发出通知由管理员决定什么时候安装这些更新程序。
- “检查更新，但是让我选择是否下载和安装更新”：仅检测是否有可用更新，并以列表形式通知管理员，由管理员决定下载和安装哪些更新程序。
- “从不检查更新(不推荐)”：关闭自动更新，此时只能使用手动更新的方式。

(3) 其他选项的含义分别如下。

- “推荐更新”：推荐更新一般不是安全更新，与系统安全性关系不大，但可以修复应用程序错误和提高系统性能。建议选中“以接收重要更新的相同方式为我提供推荐的更新”。
- “谁可以安装更新”：分配安装更新程序的权力，对于服务器，不建议选择“允许所有用户在此计算机上安装更新”。

(4) 配置完成后，单击“确定”按钮即可。

14.2　防火墙配置

在第 1 章中已经介绍了 Windows Server 2008 的基本防火墙的使用和配置方法，但这只能在一般情况下使用。虽然 Windows Server 2008 的基本防火墙安全性并不差，但是可设置选项少，功能也较少。而在服务器的使用过程中，对安全性的要求要高于普通用户，因此微软公司开发了高级安全 Windows 防火墙，并在 Windows Vista、Windows 7 和 Windows Server 2008 上配备。高级安全 Windows 防火墙与标准 Windows 防火墙相比，其安全防护能力更强，具有以下特点：

- 高级安全 Windows 防火墙是双向防火墙，它不仅可以监视、设置甚至屏蔽所有的入站连接请求(默认设置为禁止)，也可以对所有的出站连接请求进行更细致的设置(默认设置为允许)。
- 高级安全 Windows 防火墙是一种基于规则的状态防火墙，支持 IPv4 与 IPv6，远比应用层级的边界防火墙更为安全。
- 高级安全 Windows 防火墙结合了主机防火墙和 IPSec，而在 Windows XP/2003 系统中，Windows 防火墙与 IPSec 是分离的。

本节介绍微软的高级防火墙的配置方法，操作方法如下：

(1) 以管理员帐户登录 Windows Server 2008 系统后，选择“开始”→“管理工具”→“高级安全 Windows 防火墙”命令，打开 “高级安全 Windows 防火墙”窗口，如图 14-5 所示。



图 14-5　“高级安全 Windows 防火墙”窗口

其中包括入站规则、出站规则和连接安全规则 3 种规则。如果安装 Active Directory 服务，还会增加 13 条相应的安全规则。

- 入站规则。入站规则明确允许或者明确阻止与规则条件匹配的通信。例如，可以将规则配置为明确允许受 IPSec 保护的远程桌面通信通过防火墙，但阻止不受 IPSec 保护的远程桌面通信。默认情况下将阻止入站通信，若要允许通信，必须先创建相应的入站规则。在没有适用的入站规则的情况下，也可以对具有高级安全性的

Windows 防火墙所执行的操作(无论允许还是阻止连接)进行配置。

- 出站规则。出站规则明确允许或者明确拒绝来自与规则条件匹配的计算机的通信。例如，可以将规则配置为明确阻止出站通信通过防火墙到达某一台计算机，但允许同样的通信到达其他计算机。默认情况下允许出站通信，因此必须创建出站规则来阻止通信。
- 连接安全规则。包括“允许连接规则”、“拒绝连接规则”，用于允许或拒绝远程用户连接到 Windows Server 2008，强化主机安全。

入站规则、出站规则负责如何处理传入和传出的请求。在默认情况下，管理员在服务器上安装的是微软公司提供的网络服务，则防火墙会自动添加相应的规则，不需要人工干预。如果安装的是其他组织提供的网络服务或应用程序，则需要管理员根据服务访问网络的需要添加相应的出站规则和入站规则。

管理员可以通过两种方式启用或禁用防火墙规则：windows 防火墙控制台和 netsh 命令。在高级安全 Windows 防火墙控制台中，首先选择“入站规则”或“出站规则”，然后右击相应规则，从弹出的快捷菜单中选择“禁用规则”或者“启用规则”命令，即可更改其运行状态。使用 netsh 命令启用或禁用单一规则以及规则组，用法如下。

- 启用/禁用单个规则：netsh advfirewall firewall set rule name="Rule" new enable=yes | no
- 启用/禁用规则组：netsh advfirewall firewall set rule name="RuleGroup" new enable=yes | no

例如，使用如下命令可以启用“BITS 对等缓存(RPC)”规则(默认情况是禁用的)：

netsh advfirewall firewall set rule name= "BITS Peercaching (RPC) " new enable=yes

使用如下命令可以启用“BITS 对等缓存”规则组(默认情况是禁用的)：

netsh advfirewall firewall set rule group="BITS peercaching" new enable=yes

(2) 在 Windows 防火墙控制面板中，右击“入站规则”，从弹出的快捷菜单中选择“新规则”命令，打开“新建入站规则向导”，如图 14-6 所示。



图 14-6　“新建入站规则向导”的“规则类型”选择界面

与普通 Windows 防火墙类似，该向导也提供了程序、端口等多种选项，本例选中“端口”单选按钮。

(3) 单击“下一步”按钮，进入“协议和端口”界面，如图 14-7 所示。



图 14-7　“协议和端口”界面

根据要配置的端口使用的网络协议类型选择 TCP 或 UDP，再在“特定本地端口”中输入要开放的端口。如要建立 FTP 服务器，使用的是 FTP 协议，则应选择“TCP”类型，端口输入默认的 21 端口，或输入建立 FTP 服务器时管理员指定的非默认端口。

(4) 单击“下一步”按钮，进入“操作”界面，如图 14-8 所示。

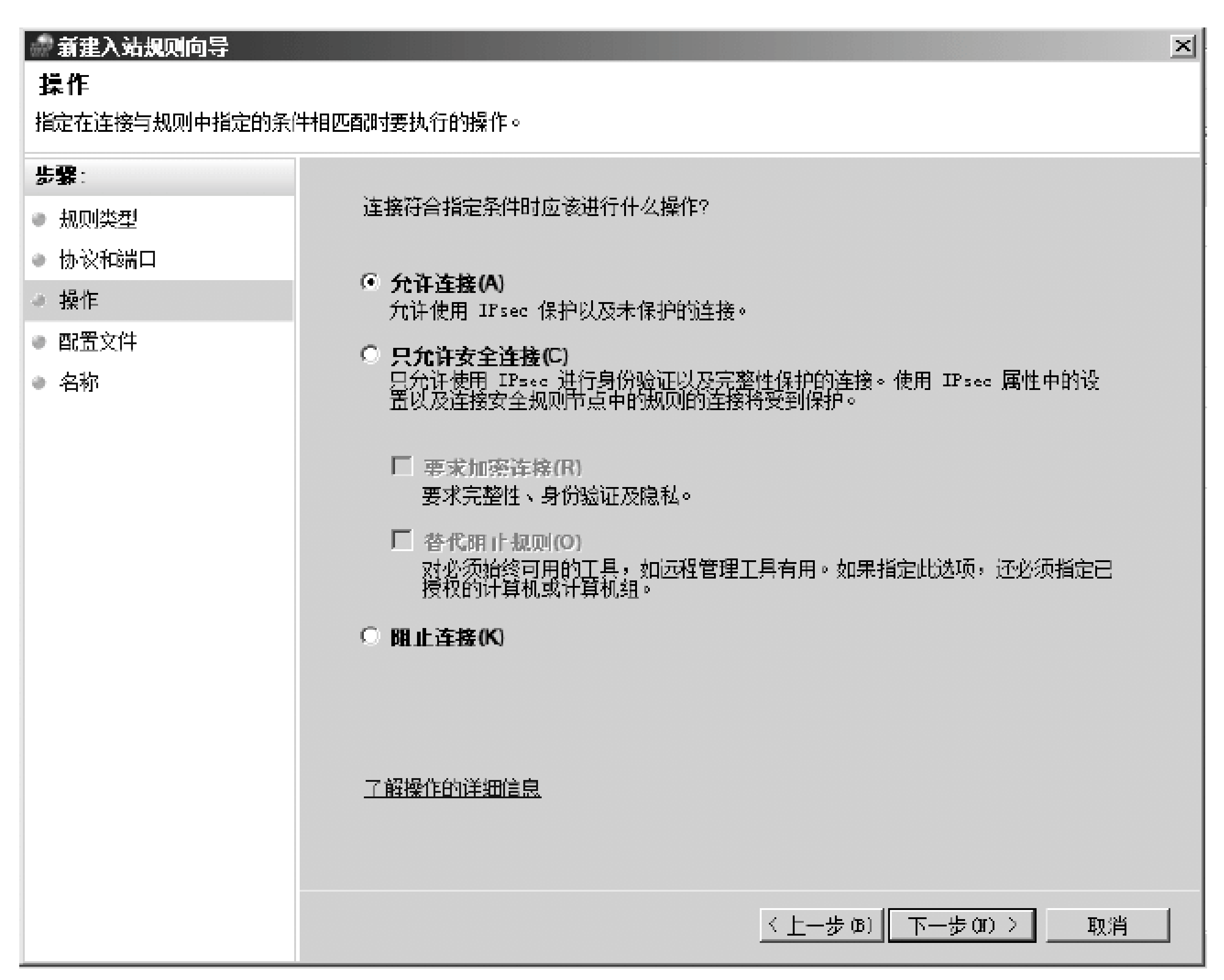


图 14-8　“操作”界面

这里有以下 3 个选项。

- 允许连接：所有用户均可使用该端口。
- 只允许安全连接：只允许特定用户访问服务器，即使用 IPSec 身份验证的用户。
- 阻止连接：不允许任何通过该端口的连接。

(5) 选中“允许连接”单选按钮，单击“下一步”按钮，进入“配置文件”界面，如图 14-9 所示。



图 14-9　“配置文件”界面

(6) 根据该服务的服务对象选择应用规则的范围，单击“下一步”按钮，进入“名称”界面，如图 14-10 所示。



图 14-10　“名称”界面

(7) 在“名称”一栏中输入该规则名称和描述信息，单击“完成”按钮即可完成规则设置，并返回高级 Windows 防火墙配置界面。出站规则设置方法与此类似，这里不再赘述。

(8) 现在即可在配置界面中看到刚添加的规则，在该规则上右击，在弹出的快捷菜单中选择“属性”命令，打开该规则的“属性”对话框，如图 14-11 所示。



图 14-11　“FTP 端口属性”对话框的“常规”选项卡

(9) 在“常规”选项卡中，可以设置该规则的名称、描述信息、是否启用和允许的连接的用户范围。

打开“程序和服务”选项卡，如图 14-12 所示。



图 14-12　“程序和服务”选项卡

(10) 在“程序”选项组中，可以选中“所有符合指定条件的程序”单选按钮，使所有程序都可以使用该规则，也可以选中“此程序”单选按钮，指定某个软件才能使用该规则；在“服务”选项组中可以选择哪些服务可以使用该规则，默认为所有服务均可。

打开“用户和计算机”选项卡，如图 14-13 所示。

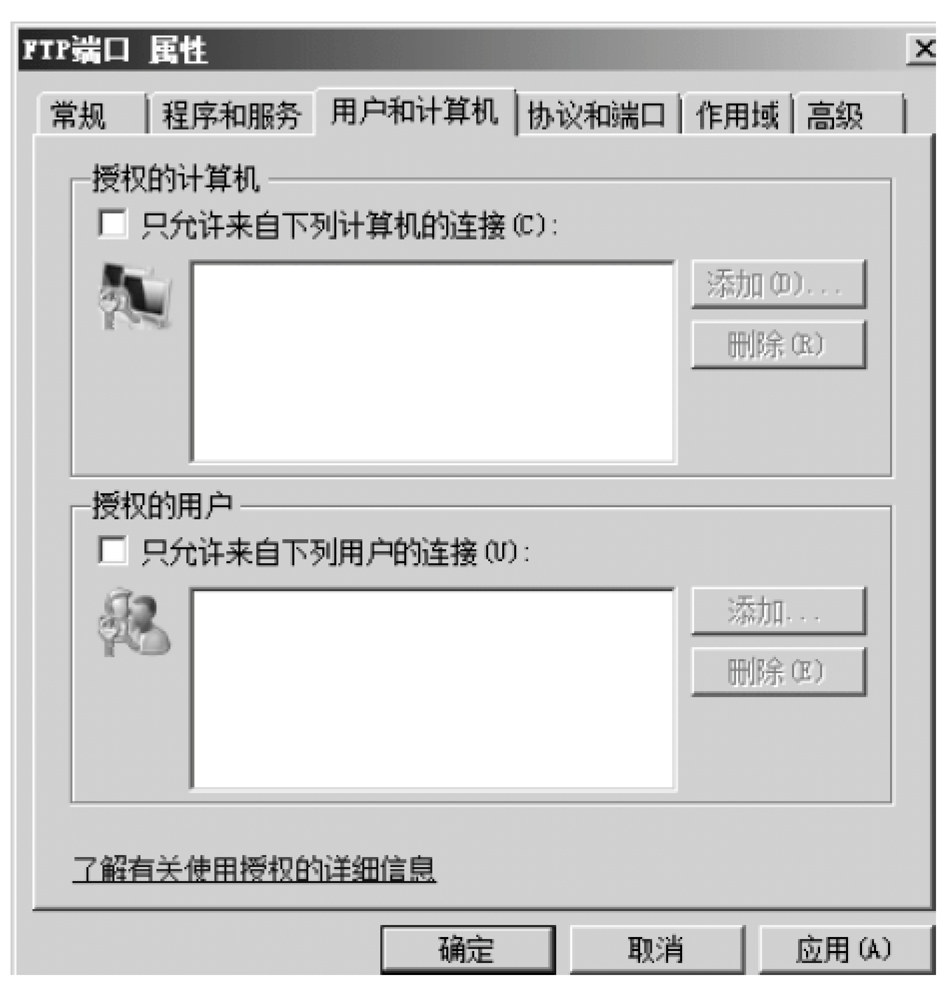


图 14-13　“用户和计算机”选项卡

(11) 只有在“常规”选项卡中选中“只允许安全连接”单选按钮才能使用该选项卡中的选项，可以只允许特定 IP 地址的计算机或以本机特定用户的身份使用该规则。

打开“协议和端口”选项卡，如图 14-14 所示。



图 14-14　“协议和端口”选项卡

(12) 在该选项卡中可以设置定义规则的协议类型，本地端口和远程端口。远程端口是指访问服务器的请求是从哪个端口发出的，一般设置为“所有端口”。ICMP 选项一般是不可用的，如果管理员设置的协议类型为“TCMP v15”，则该选项可用，并可以设置远程计算机使用 ping 命令尝试连接服务器时是否给予应答。

打开“作用域”选项卡，如图 14-15 所示。

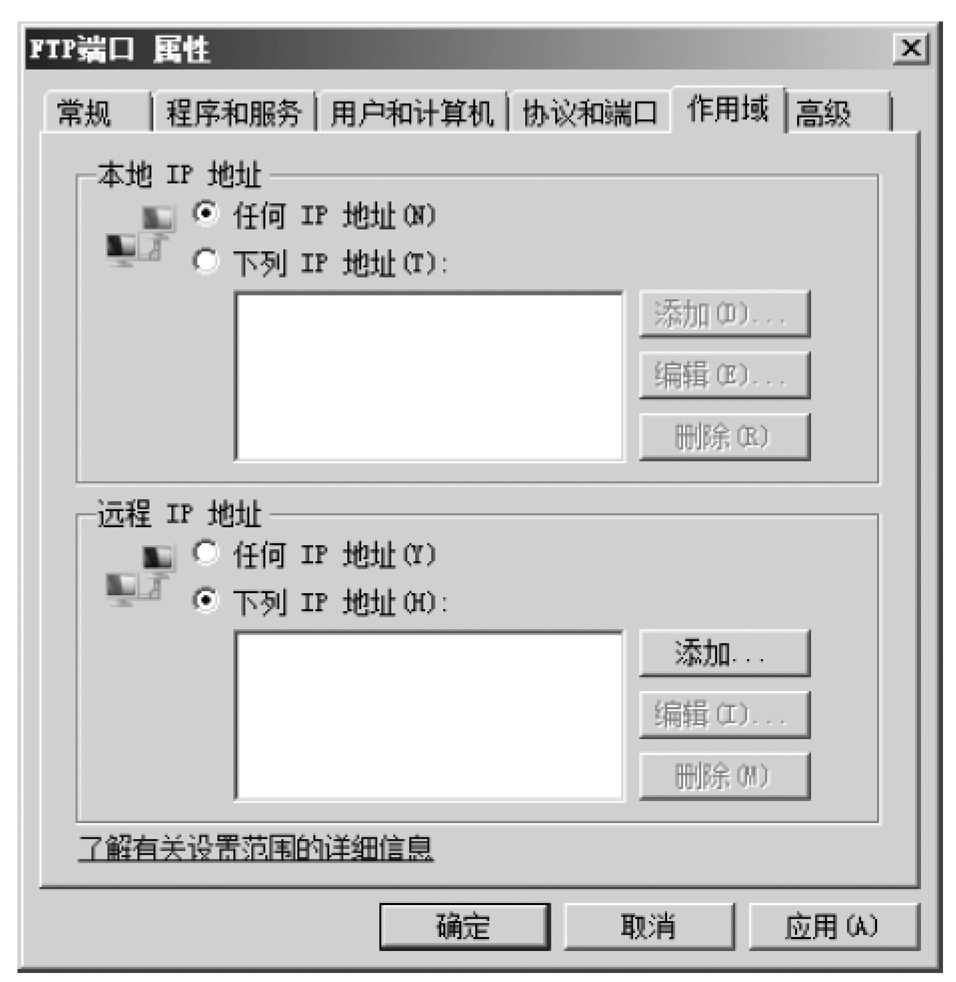


图 14-15　“作用域”选项卡

(13) 作用域是入站或出站防火墙规则的本地和远程地址。使用作用域为规则指定代表本地计算机或远程计算机 IP 地址的 IP 地址、范围、子网或关键字(只用于远程计算机)。然后，该规则被用于任何同时满足规则中其他标准的本地和远程地址之间的任何连接。通过该选项可以选定本机提供服务的 IP 地址和允许访问服务器的计算机的 IP 地址。

打开“高级”选项卡，如图 14-16 所示。

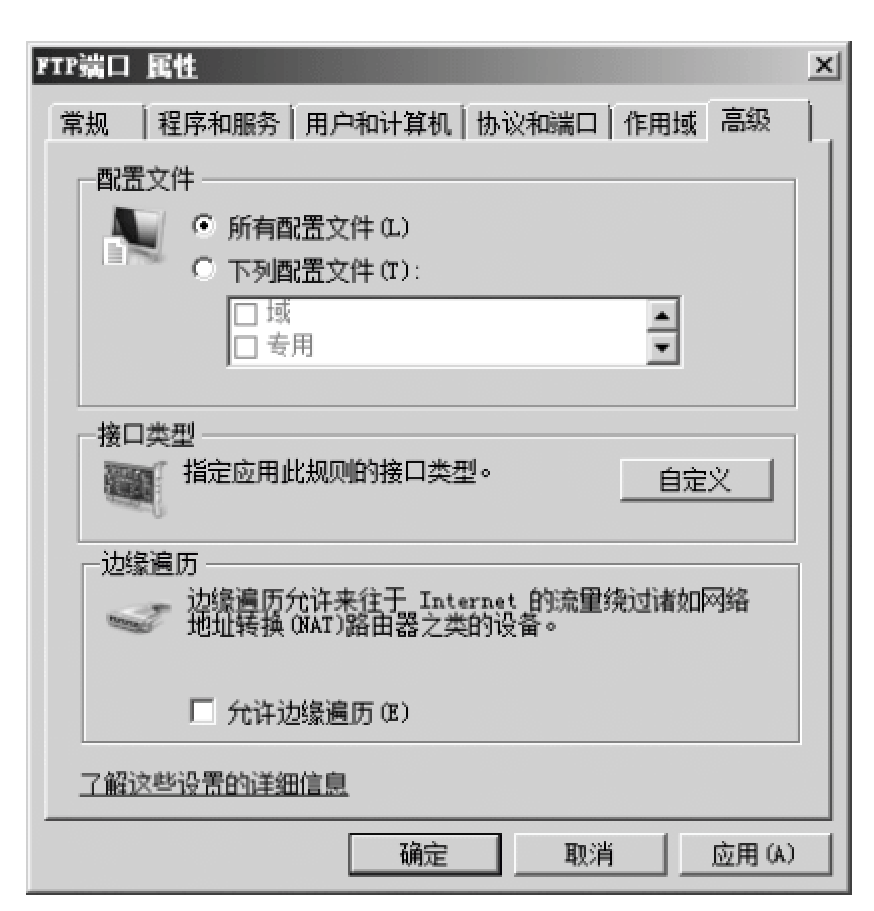


图 14-16　“高级”选项卡

(14) “配置文件”选项组用于设置该规则的应用范围；“接口类型”选项组用于配置该规则应用于什么样的网络连接，有局域网、无线网络、远程访问和所有类型 4 种；选中“允许边缘遍历”单选按钮，将可以不通过 NAT 或从边缘设备对应用该规则的应用程序、服务或端口进行全局寻址和访问。配置完成后，单击“确定”按钮即可完成规则属性修改并使之生效。

14.3　防病毒配置

计算机病毒就是利用计算机软件与硬件的缺陷，由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。

计算机技术在近几十年的高速发展，也使得计算机病毒技术越来越先进，病毒带来的损失也越来越大，近些年来已达到每年损失上百亿美元。

计算机病毒大多是利用计算机软件的漏洞破坏计算机系统，而且计算机病毒有其自身的规律，因此如果管理员可以对计算机系统进行合理的设置，采取必要的措施，可以减少被计算机病毒攻击的机会。

Windows Server 2008 本身已经是非常安全的系统，但仍然会受到病毒的侵袭。为了进一步提高系统的安全性，Windows Server 2008 内置了数据执行保护功能(DEP)。数据执行保护功能最早出现自 Windows XP 的 SP2 更新程序。该功能可以监视内存中的指定区域，这些区域是专为系统文件而设，因此只要发现有程序访问这些被保护的内存空间，就认为是恶意代码在运行，然后禁止这些代码执行。DEP 不能判定一个程序是否为病毒，但是可以禁止危害被保护内存空间的程序运行。

Windows Server 2008 作为一个网络操作系统，主要运行的是其自带的一些软件，如 IIS 等，很少使用其他软件，因此本身的数据执行保护功能是被关闭的。如要打开数据执行保护功能，选择“开始”→“运行”命令，然后在打开的对话框中输入 cmd 命令(不含引号)，按回车键，打开命令提示符工具，输入命令 bcdedit.exe /set {current} nx AlwaysOn，然后按回车键，如图 14-17 所示。

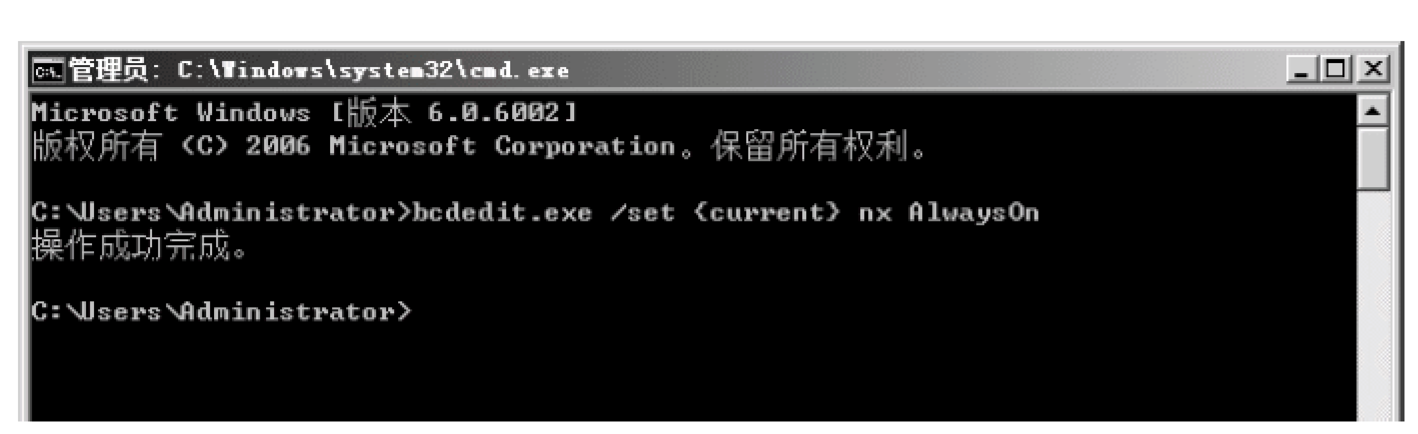


图 14-17　命令提示符工具界面

如果看到提示“操作成功完成”，则说明数据执行保护功能已经成功打开。

由于数据执行保护功能无法判断一个程序是否为病毒，因此它不能处理所有的病毒攻击。为了使系统更加安全，最好为系统安装杀毒软件，本章节使用微软公司开发的 MSE(Microsoft Security Essentials)免费杀毒软件为例。

使用杀毒软件的方法如下：

(1) 从微软网站下载 MSE，双击下载的软件，根据安装向导提示安装 MSE。需要注意的是，MSE 在安装过程中要进行正版验证，只提供给正版软件用户使用。

(2) 安装完毕后，计算机会重新启动，重启后 MSE 会自动进行病毒库的更新并进行一次快速扫描。

(3) 在桌面的通知区域的 MSE 图标上右击，在弹出的快捷菜单中选择“打开”命令，如图 14-18 所示。



图 14-18　MSE 托盘图标的右键快捷菜单

(4) 选择该命令后，打开 MSE 主界面，如图 14-19 所示。



图 14-19　MSE 主界面

(5) 在“主页”选项卡中，可以对计算机进行扫描。MSE 共有以下 3 种扫描模式。

- 快速：在该模式下只扫描最可能感染病毒的文件，扫描速度快、耗时短，但是可能会导致一些病毒扫描不出来。这种模式适合一般性的病毒扫描。
- 完全：在该模式下 MSE 扫描计算机中所有的文件，能够最大限度地查找计算机中被感染的文件，但是由于扫描量大，导致速度慢、耗时较长。这种模式适合全面对计算机进行检查。
- 自定义：在该模式下可以由用户选择对哪个分区和文件夹进行扫描，自由度较高，该模式适合于对计算机能够熟练操作的用户使用。

选择好合适的扫描模式后，单击“立刻扫描”按钮就可以开始扫描计算机。

(6) 打开“更新”选项卡，如图 14-20 所示。



图 14-20　“更新”选项卡

(7) 单击“更新”按钮，MSE 会连接到微软网站上升级病毒库，以便 MSE 可以查杀最新出现的各种病毒和间谍软件。打开“历史记录”选项卡，如图 14-21 所示。



图 14-21　“历史记录”选项卡

(8) 该界面显示了所有以往检测到的潜在的威胁。打开“设置”选项卡，如图 14-22 所示。



图 14-22　设置“计划扫描”界面

(9) 当前显示的是“计划扫描”选项，用于设置定时扫描。选中“在我的计算机上运行计划扫描(推荐)”复选框，然后可以在“扫描类型”下拉列表中选择扫描病毒的扫描类型；在“每周”下拉列表中选择每周中哪一天进行病毒扫描；在“时间”下拉列表中选择扫描的时间。其余选项保持默认设置，然后单击“保存更改”按钮保存扫描计划。单击左侧窗口中的“默认操作”，打开“默认操作”设置界面，如图 14-23 所示。

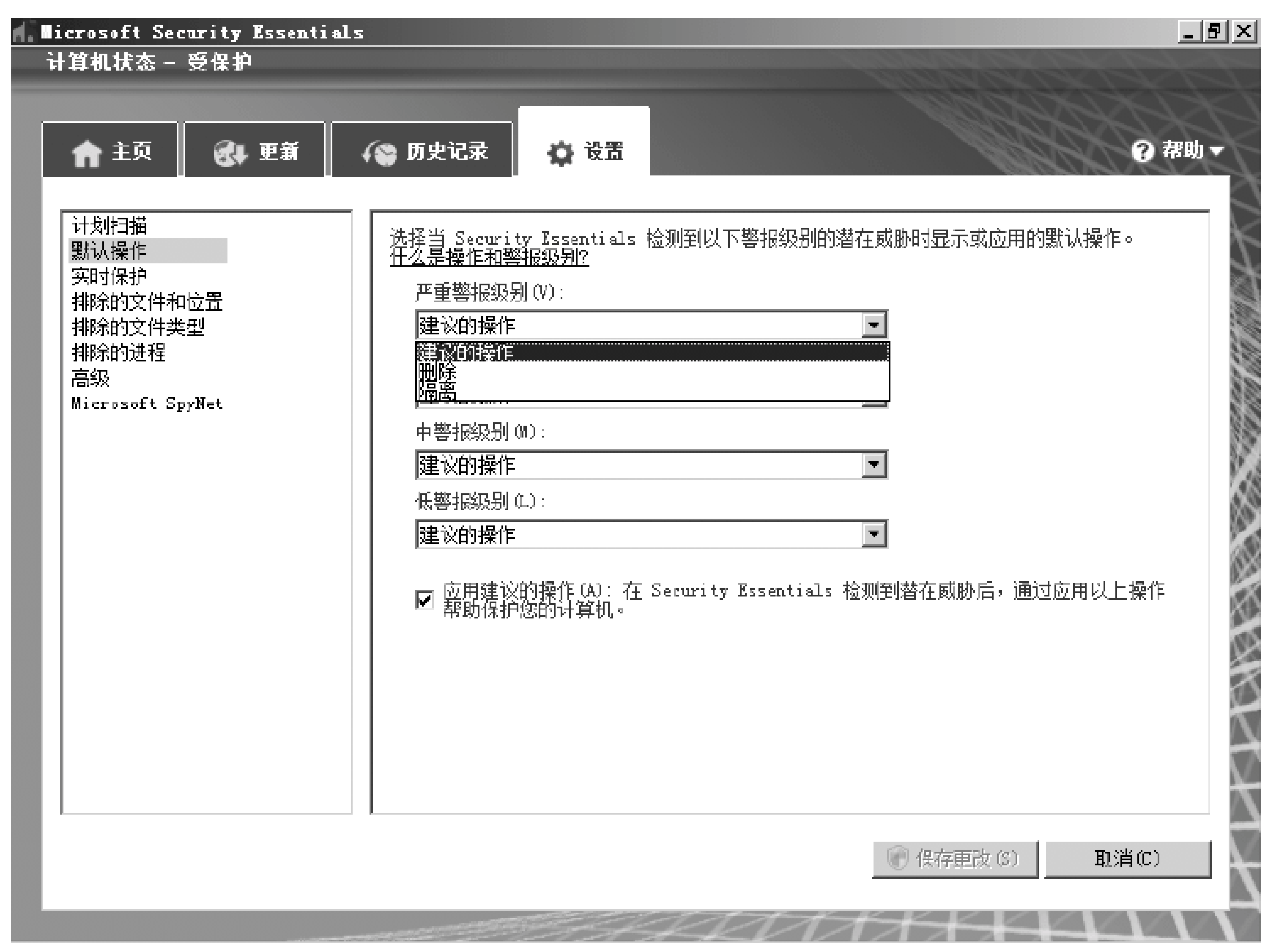


图 14-23　“默认操作”设置界面

(10) 在该界面中，MSE 将有潜在危害的文件分为 4 个等级：严重警报级别、高警告级别、中警告级别、低警报级别。对于有潜在危害的文件，可以有两种操作：删除和隔离。如果选择删除操作，发现了有危害的文件，直接删除掉；如果选择隔离操作，有潜在危害的文件会被移动到一个指定区域，正常情况下用户将无法访问，以等待下一步处理。设置完毕后单击“保存更改”按钮完成设置。单击左侧窗口中的“实时保护”，打开“实时保护”设置界面，如图 14-24 所示。



图 14-24　“实时保护”设置界面

(11) “实时保护”用于设置对哪些文件和行为进行监控，以便出现问题后立刻可以发现和处理。

(12) 左侧窗口中的“排除的文件和位置”、“排除的文件类型”和“排除的进程”3项用于设置在监控和扫描过程中，哪些位置的文件、哪些类型的文件和哪些可执行文件不被扫描和监控。这样做可以提高扫描速度，如果对计算机操作不够熟悉，不要设置这些选项。

(13) 单击左侧窗口中的“高级”，打开“高级”设置界面，如图 14-25 所示。



图 14-25　“高级”设置界面

(14) 各选项含义如下。

- 扫描存档文件：扫描压缩文件包以查找被压缩的文件中是否包含病毒。
- 扫描可移动驱动器：当使用完全扫描模式时，如果连接有可移动驱动器，如优盘、移动硬盘等，也一同扫描。
- 创建系统还原点：在删除有危害的文件之前，先创建一个系统还原点以便还原。
- 允许所有用户查看完整的历史记录结果：允许本机上管理员和非管理员帐户查看“历史记录”选项卡中的历史检测记录。
- 在以下时间后删除隔离文件：一些文件如果被认为是有潜在危害的，可以选择将其隔离起来，但是这样会占用一些磁盘空间。可以选择定时删除这些隔离文件以释放磁盘空间。

更改设置后，单击“保存更改”按钮以保存设置。

(15) 单击左侧窗口中的 Microsoft SpyNet，打开 Microsoft SpyNet 设置界面，如图 14-26 所示。



图 14-26　“Microsoft SpyNet”设置界面

(16) Microsoft SpyNet 是一个连接社区，可以接收来自用户提供的信息，通过分析这些信息，可以为用户提供最新的病毒库和处理意见。各选项含义如下。

- 我不想加入 SpyNet：不向外界发送任何信息，但也无法接收任何信息。
- 基本成员身份：Security Essentials 向 Microsoft 发送有关 Security Essentials 检测到的软件的基本信息，包括软件来源、用户的操作或 Security Essentials 自动应用的操作以及这些操作是否成功执行。
- 高级成员身份：除基本信息外，Security Essentials 还会向 Microsoft 发送有关恶意软件、间谍软件和可能不需要的软件的更多信息，包括软件位置、文件名、软件操作方式以及软件影响计算机的方式。

在默认状态下，用户以“基本成员资格”加入 Microsoft SpyNet 社区，如果不确定哪种方式更好，可以保持默认设置。

但是，由于目前杀毒软件的技术还不能查杀未知病毒，只能从已知病毒中提取特征码，然后杀毒软件从网上获取这些特征码，这样杀毒软件才可以根据特征码查杀病毒。虽然目前许多杀毒软件公司也在开发一些新的技术，以应对新出现的病毒甚至是未知的病毒，但是这些技术都存在各种问题而达不到实用程度，因此特征码查杀仍是目前杀毒软件使用的主要手段。由于技术原因，即使计算机上安装了杀毒软件，如果出现了新病毒，或者病毒库更新不及时，都会导致无法处理某些病毒的侵袭。因此，管理员不仅要做好杀毒软件的及时更新，还要养成一些良好的习惯：

- 认真设置 NTFS 权限，不要让无关用户尤其是 EveryOne 用户获得过高的权限。
- 不要使用未经验证的软件。
- 不要随意使用移动存储设备，如果一定要使用移动存储设备，一定要在安全的主机上查杀病毒后再在服务器上使用。
- 尽量不要使用服务器上网或下载文件。
- 认真设置防火墙，这样即使被病毒侵袭也能阻止进一步感染或信息被泄露。

● 设置杀毒软件为自动更新，最好是每天更新至少一次，并根据情况及时手动更新，以及定期全盘杀毒。

如果有良好的使用习惯，再配合杀毒软件，可以大大减少被病毒侵袭。

14.4 防间谍配置

间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。它能够削弱用户对其使用经验、隐私和系统安全的物质控制能力；使用用户的系统资源，包括安装的程序；或者搜集、使用、并散播用户的个人信息或敏感信息。

“间谍软件”应该说是一个灰色区域，所以并没有一个明确的定义。然而，正如同名字所描述的一样，它通常被泛泛地定义为从计算机上搜集信息，并在未得到该计算机用户许可时便将信息传递到第三方的软件，包括监视击键、搜集机密信息(密码、信用卡号、PIN码等)、获取电子邮件地址、跟踪浏览习惯等。间谍软件还有一个副作用，在其影响下这些行为不可避免的会影响网络性能，降低系统速度，进而影响整个系统。

间谍软件之所以成为灰色区域，主要因为它是一个包罗万象的术语，包括很多与恶意程序相关的程序，而不是一个特定的类别。大多数间谍软件的定义不仅涉及广告软件、色情软件和风险软件程序，还包括许多木马程序，如 Backdoor Trojans，Trojan Proxies 和 PSW Trojans 等。这些程序早在 10 年前第一个 AOL 密码盗取程序出现时就已经存在，只是当时还没有“间谍软件”这个术语。

间谍软件的另外一个附属品就是广告软件。此时，间谍软件以恶意后门程序的形式存在，该程序可以打开端口、启动 FTP 服务器、或者搜集击键信息并将信息反馈给攻击者。间谍软件可以存在于合法的(并可接受的)商业应用程序中，可以给网络管理员在影响和监视系统方面很大的权力。

尽管这些程序并非很新，但近年来有恶意目的的程序却不断增加，引起媒体和反间谍软件开发商的很大关注。

虽然 Windows Server 2008 是网络操作系统，被间谍软件侵袭的机会不多，但是一旦服务器被侵袭，危害将是非常大的。因此服务器也要非常重视防间谍软件。

有不少杀毒软件也可以查杀间谍软件，但是许多间谍软件仅仅是较轻地危害计算机系统，给用户带来了一定的损失，但是达不到病毒的危害程度，因此很多杀毒软件对间谍软件检测不很严格，会放过一些间谍软件。因此安装专用的反间谍软件还是很有必要的。

微软公司为自己的 Windows 系统开发了恶意软件删除工具。该工具可以在一定程度上保护系统不受间谍软件的侵害。具体使用方法如下：

(1) 微软恶意软件删除工具是作为补丁程序在 Windows Update 上发布的，因此只要打开自动更新功能，系统就会自动安装该工具。

(2) 选择“开始”→“运行”命令，在打开的“运行”对话框中输入 mrt 命令(不含引号)，然后单击“确定”按钮，打开微软恶意软件删除工具，如图 14-27 所示。

(3) 单击“下一步”按钮，进入“扫描类型”界面，如图 14-28 所示。

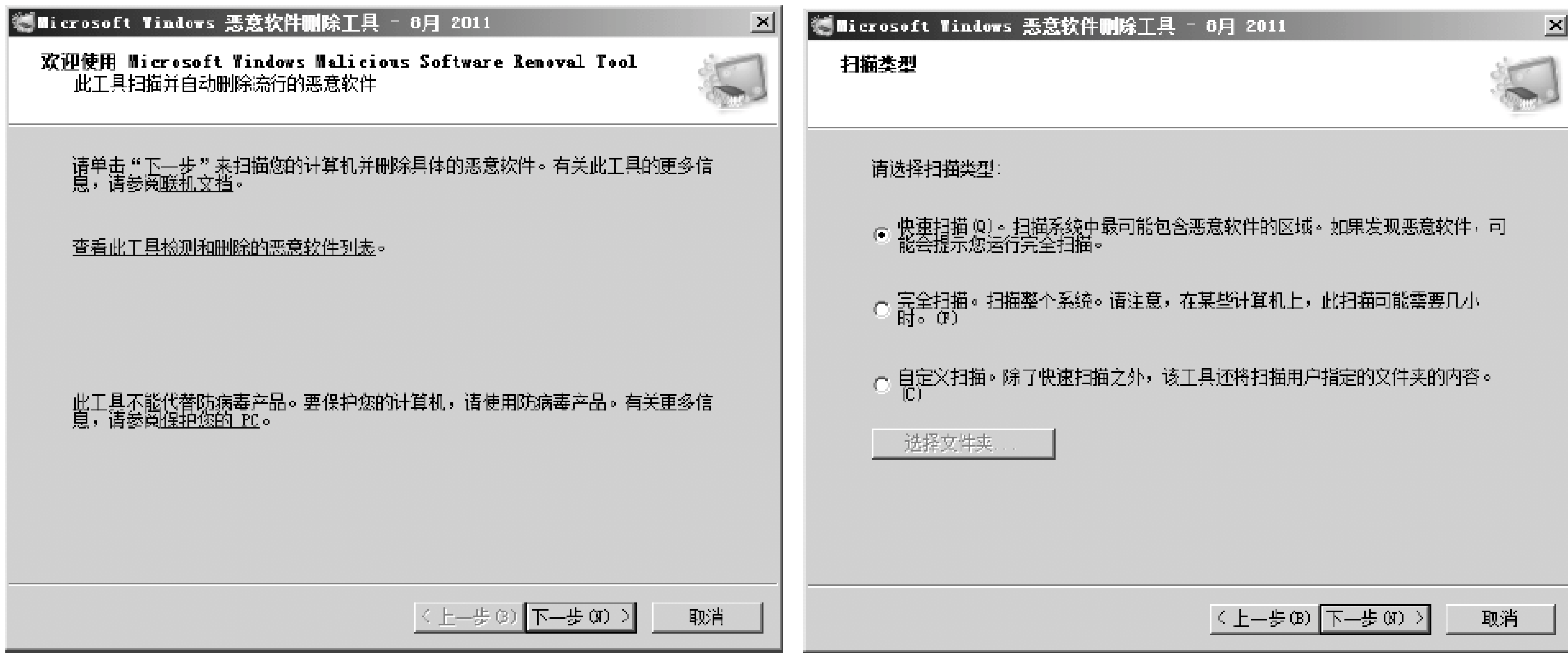


图 14-27　微软恶意软件删除工具启动界面　　图 14-28　“扫描类型”选择界面

(4) 在该界面可以选择扫描的类型，共有“快速扫描”、“完全扫描”和“自定义扫描”3 种模式，根据需要选择合适的模式后，单击“下一步”按钮开始扫描，如图 14-29 所示。

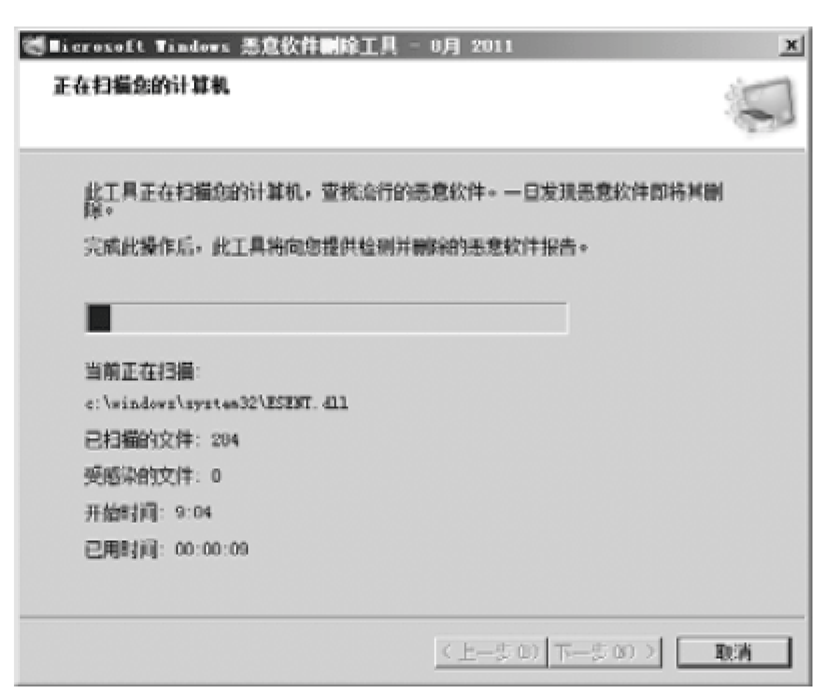


图 14-29　扫描界面

(5) 扫描完毕后，显示扫描结果，如图 14-30 所示。如果没有任何有危害的文件，单击“完成”按钮退出即可；如果有恶意软件，会显示文件列表和建议的处理方法供选择。



图 14-30　扫描结果报告界面

微软恶意软件删除工具使用简单，但是更新不及时，在效率上不及更加专业的防间谍软件。

SuperAntiSpyware 是一款优秀的防间谍软件，受到广大专家和用户的好评。SuperAntiSpywar 还开发有免费版本，方便个人用户的使用。SuperAntiSpywar 的安装和使用方法如下：

(1) 从网上下载 SuperAntiSpyware 的安装文件，然后双击该文件并按照安装向导提示进行安装。需要注意的是，该软件的软件安装界面为英文，在安装结束的时候可以选择使用时软件界面采用的语言，如图 14-31 所示。

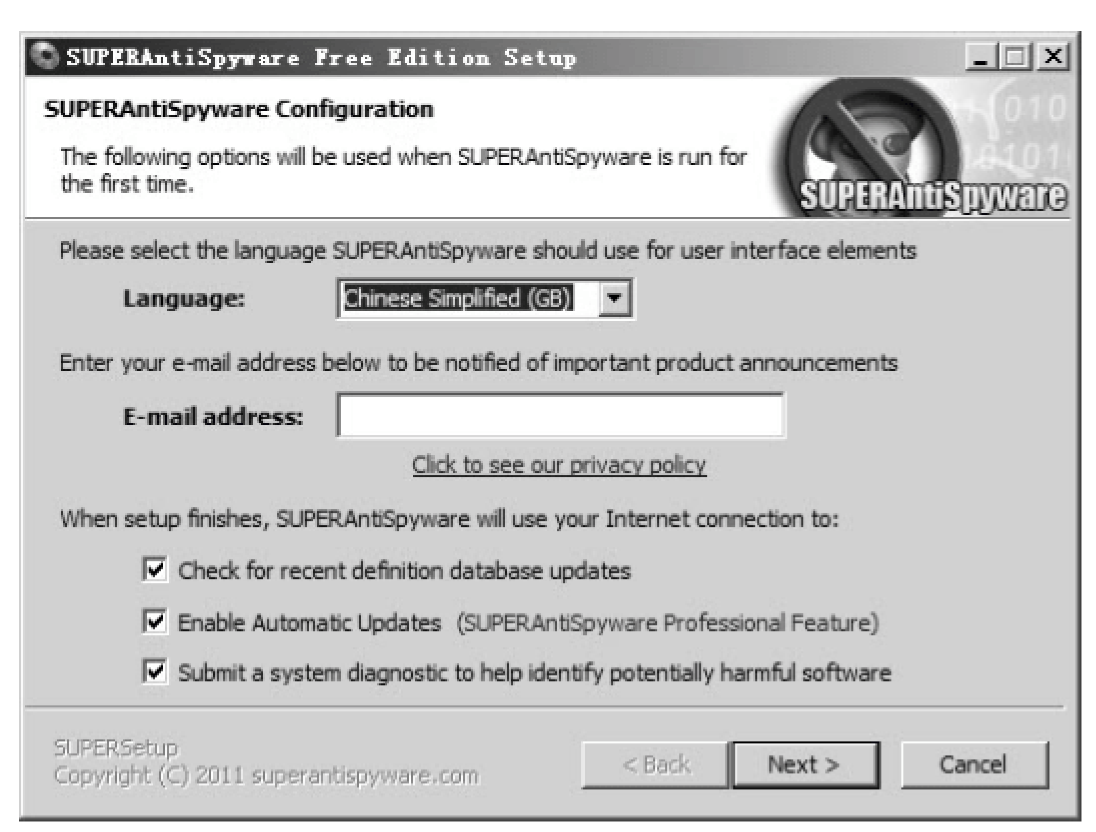


图 14-31　安装启动界面

(2) 在 Language 下拉列表中选择 Chinese Simplified(GB)。其余的操作请按照向导提示进行。完成安装后，第一次启动 SuperAntiSpyware 时，软件会自动联网进行升级，但是此时软件界面仍是英文，如图 14-32 所示。

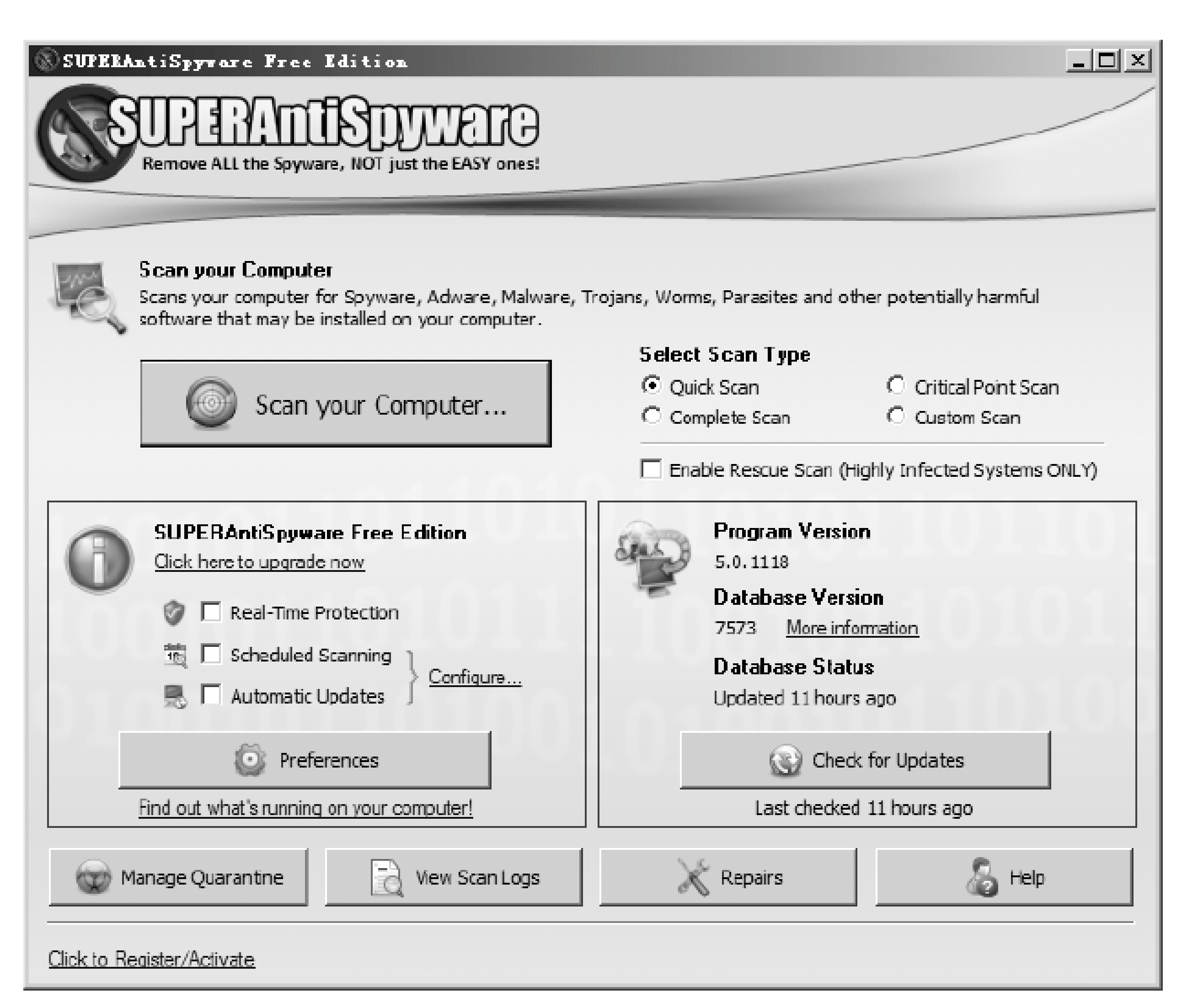


图 14-32　软件主界面

(3) 单击界面中的 Preference 按钮，打开 Scanning and Program Preferences 界面，在其中的 Language 下拉列表中选择 Chinese Simplified(GB)选项，如图 14-33 所示。

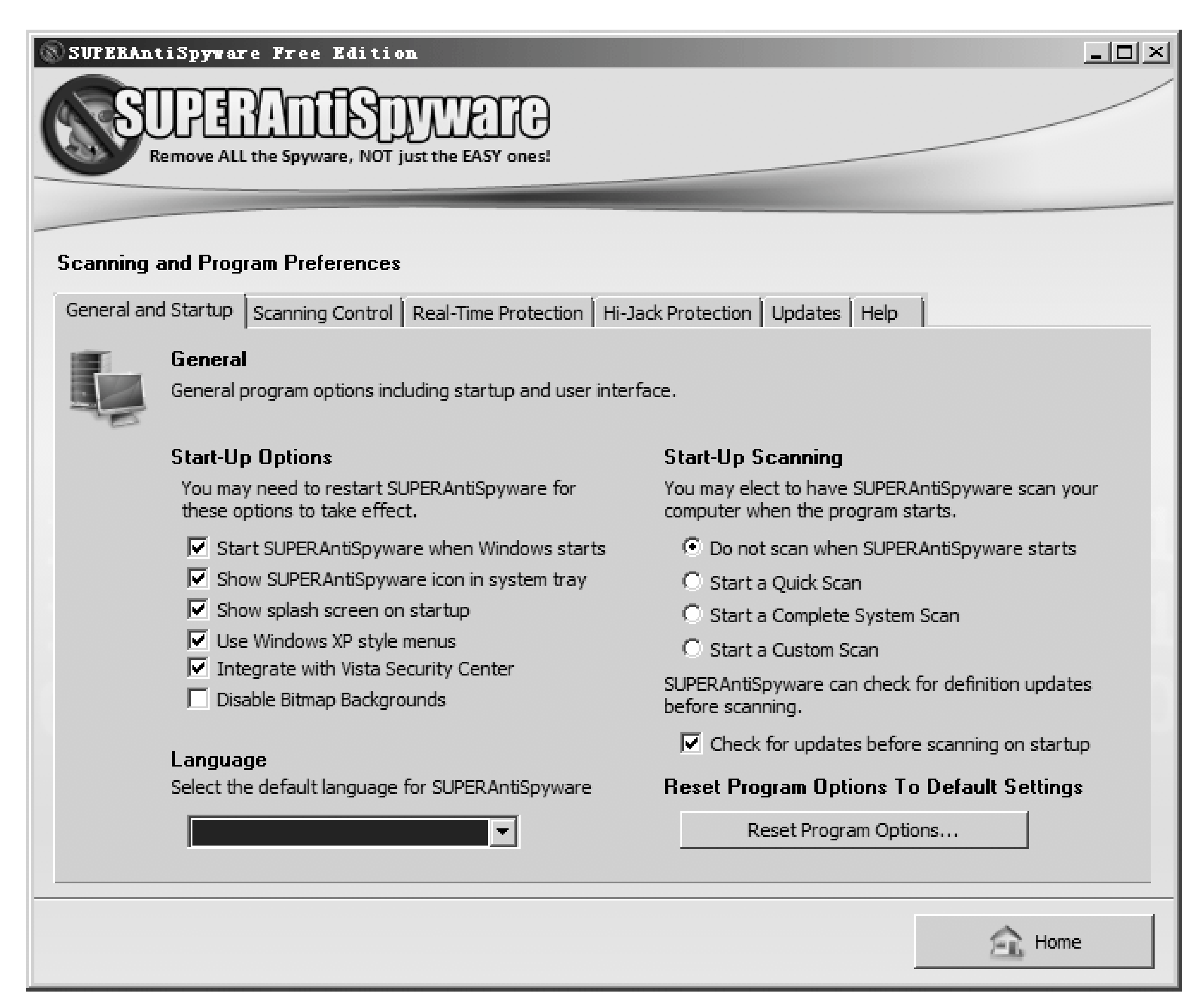


图 14-33　Scanning and Program Preferences 界面

(4) 选择完后，软件界面将转换为简体中文界面，单击 Home 按钮返回主界面，如图 14-34 所示。



图 14-34　软件中文主界面

(5) 由于是免费版本，因此“实时保护”、Scheduled Scanning(计划扫描)和 Automatic Updates(自动升级)3 个功能不能使用，如果想使用这些功能，单击 Click here to upgrade now 选项将软件升级到专业版。

(6) 单击 Check for Update 按钮，打开升级对话框，如图 14-35 所示。这时 SuperAntiSpyware 可以连接到网站进行升级一边查杀最新的间谍软件。升级完毕后，单击“完成”按钮关闭升级对话框。

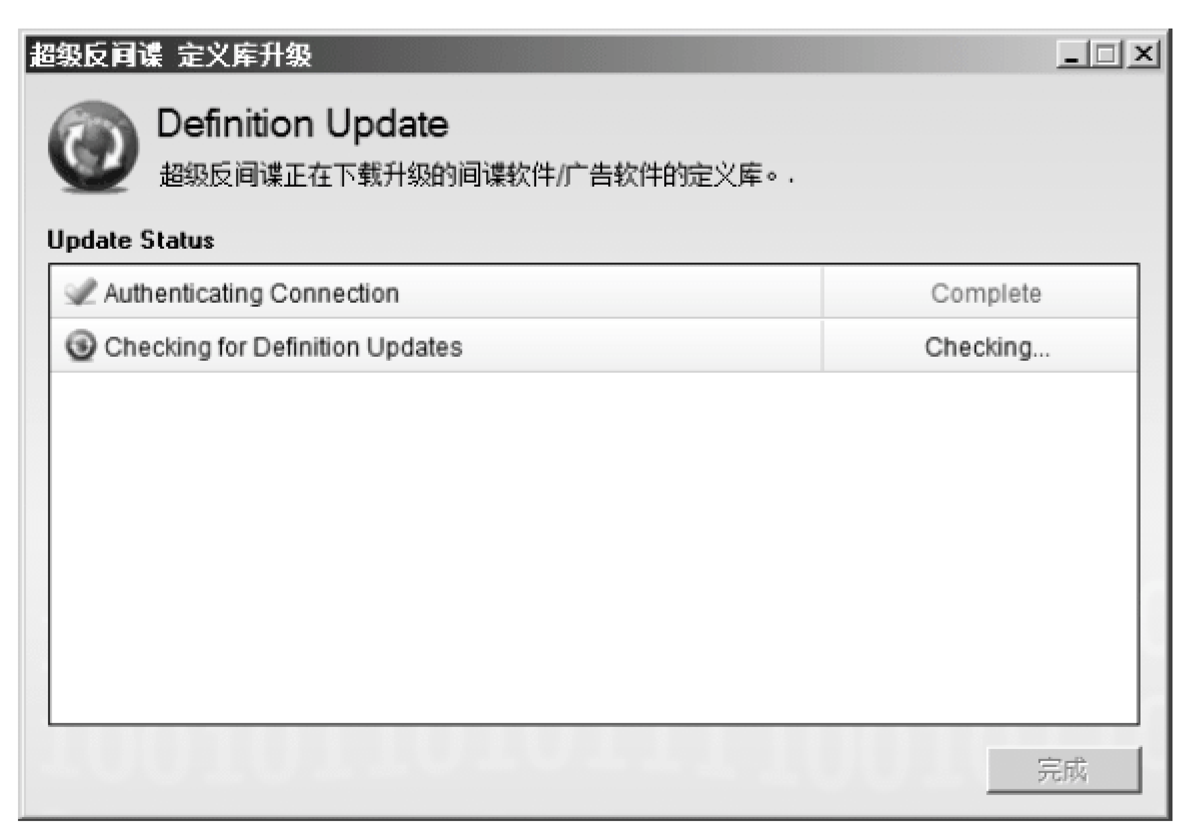


图 14-35　升级对话框

(7) 软件界面上方是扫描选项，SuperAntiSpyware 有 Quick Scan(快速扫描)、Critical Point Scan(关键点扫描)、Complete Scan(完全扫描)和 Custom Scan(自定义扫描)4 种模式，根据需要选择合适的模式，单击“扫描您的电脑”按钮，开始对系统进行扫描。扫描完毕后，如果有间谍软件则列出找到的间谍软件，如果没有任何问题，弹出扫描汇总对话框，如图 14-36 所示。单击 OK 按钮返回主界面。

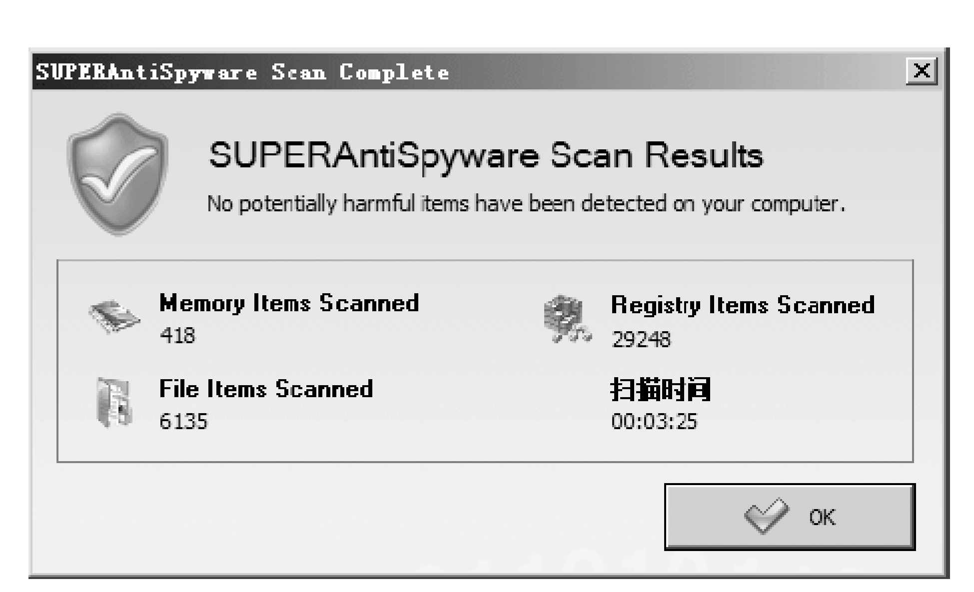


图 14-36　扫描汇总对话框

(8) 单击界面中的 Preference 按钮，打开 Scanning and Program Preferences 界面，在“常规选项和启动选项”选项卡中可以设置启动系统时和启动软件时可以执行的操作，如图 14-37 所示。

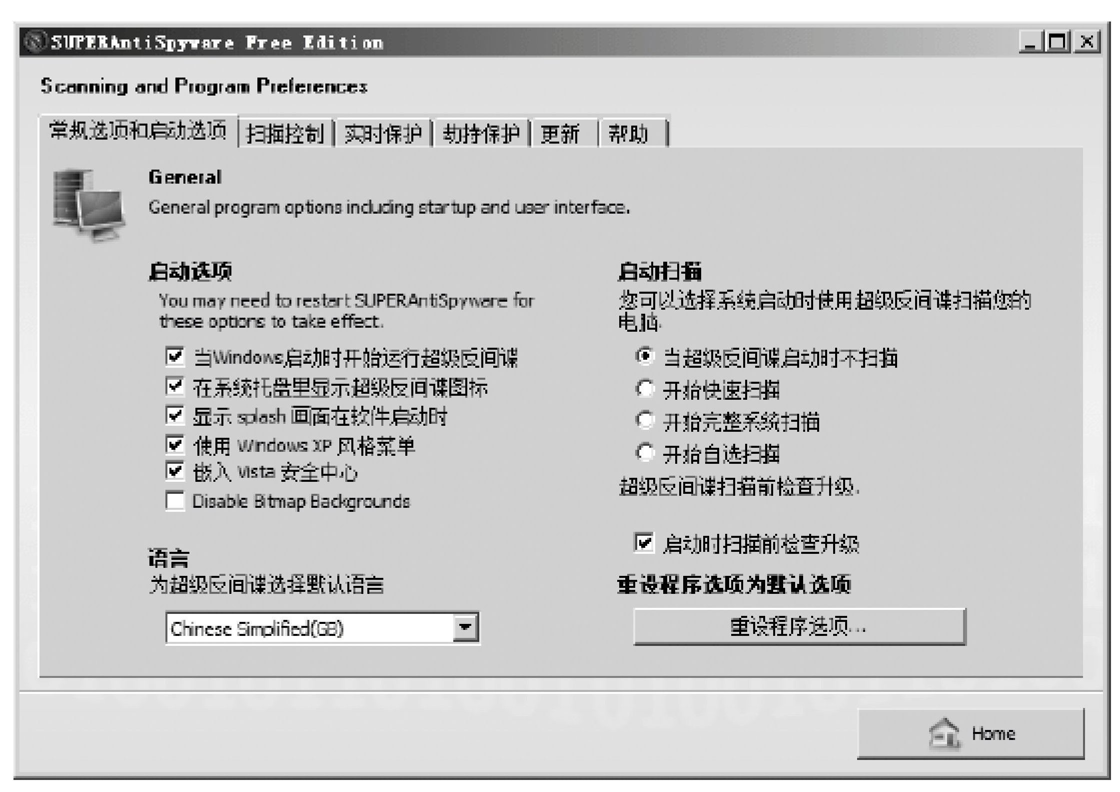


图 14-37 “常规选项和启动选项”选项卡

(9) 打开“扫描控制”选项卡，如图 14-38 所示。在该选项卡中，可以设置软件扫描过程中可以使用的模式和要扫描的文件类型。

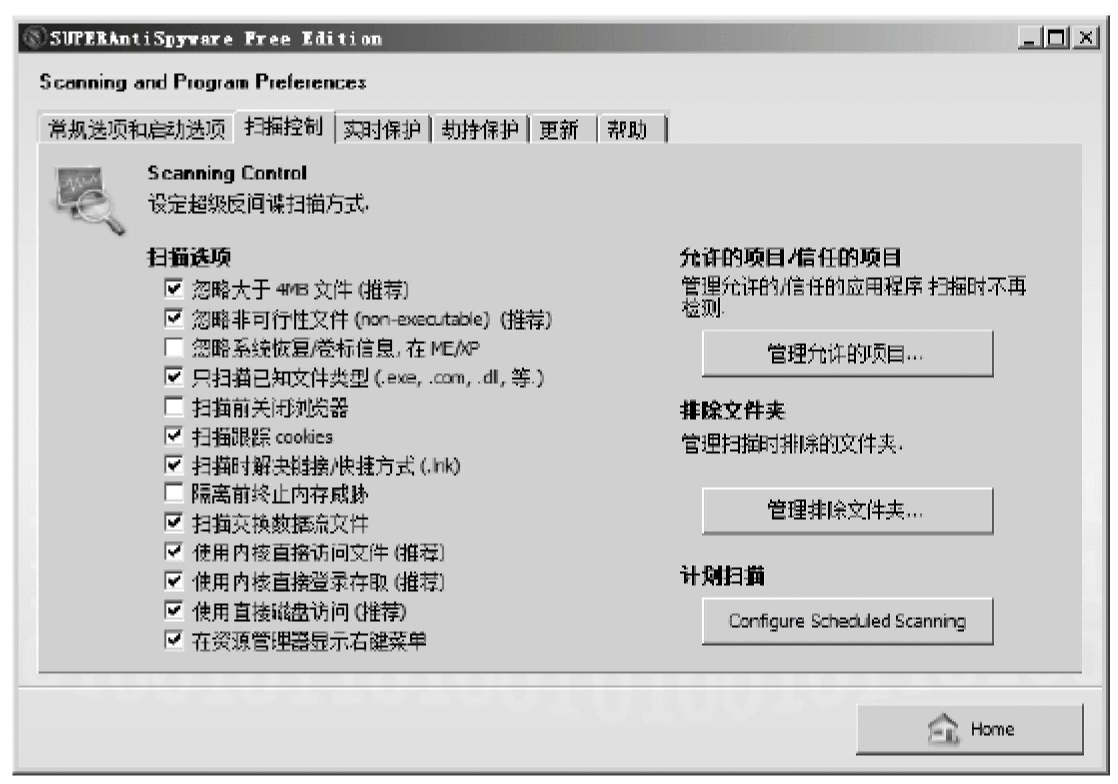


图 14-38 “扫描控制”选项卡

(10) 打开“劫持保护”选项卡，如图 14-39 所示。在该选项卡中可以设置对 IE 浏览器进行保护。



图 14-39 “劫持保护”选项卡

(11) 设置完毕后，单击 Home 按钮返回主界面。单击主界面上的“修复”按钮，打开“修复”界面，如图 14-40 所示。

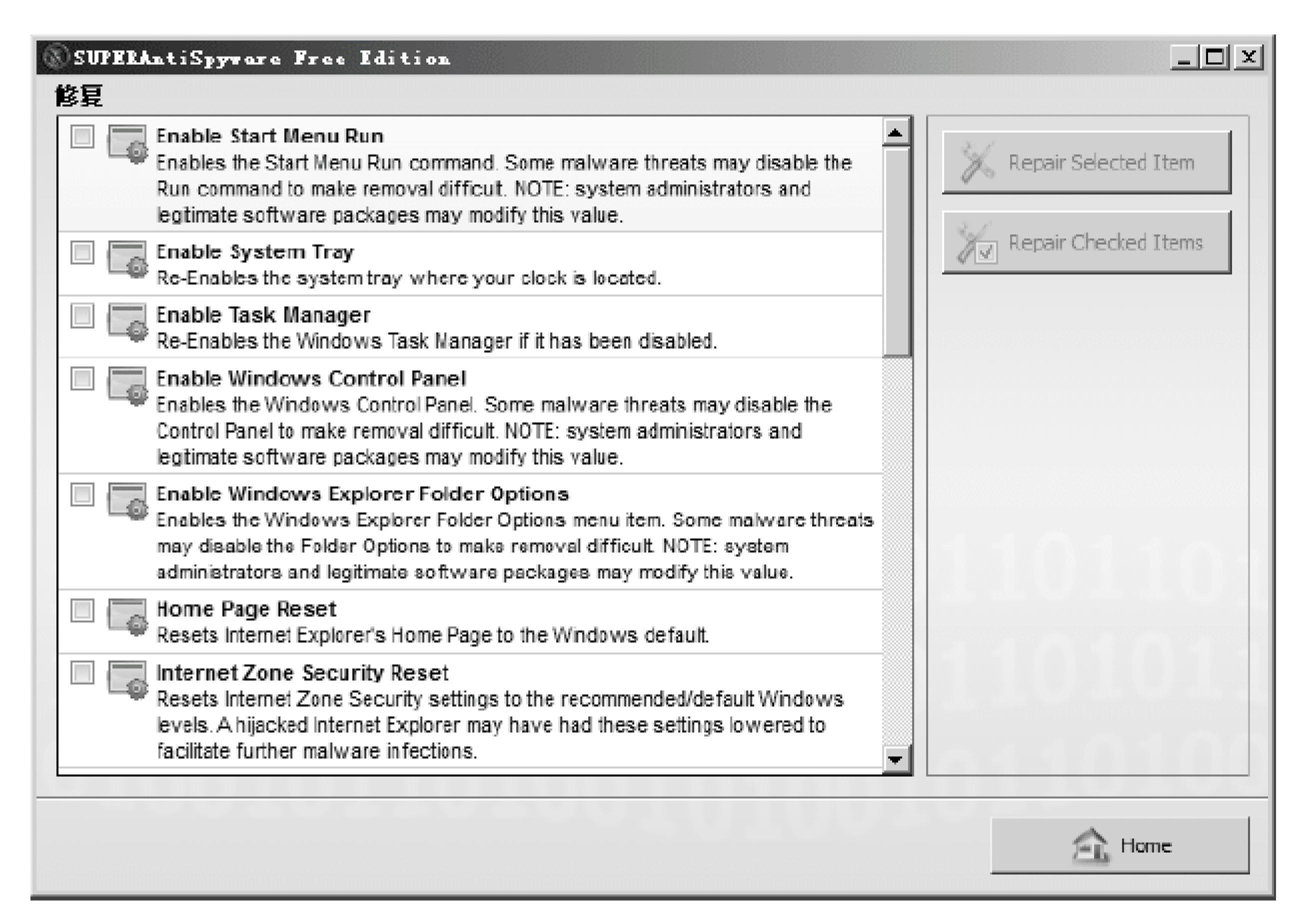


图 14-40　“修复”界面

(12) 如果系统的某些设置被篡改，可以利用修复功能进行修复。选中需修复项目前面的复选框，然后单击 Repair Selected Item 按钮，对所选项目进行修复。

通过这些软件的保护，可以大大降低系统被间谍软件侵袭的机会。

14.5　本章小结

本章介绍了提高 Windows Server 2008 系统安全性的一般方法，所有的操作系统都不可避免地出现 Bug，也都存在被攻击的可能性，但是管理员可以通过打补丁、配置防火墙、安装防病毒软件等方法提高自身安全性，降低被攻击的概率。

(1) Windows Server 2008 更新：本节介绍了常见漏洞的类型和修复漏洞的方法。

(2) Windows Server 2008 防火墙配置：本节介绍了 Windows Server 2008 中高级防火墙的使用，在高级防火墙中，管理员可以定义更加详细的规则，从应用程序到端口都可以进行设置。设置合适的防火墙规则是保证系统安全的一个重要环节。

(3) Windows Server 2008 防病毒配置：本节介绍了微软公司的杀毒软件 MSE，管理员可以使用 MSE，最大限度地保护系统不被病毒侵袭。但是防病毒软件不是万能的，需要配合其他安全设置才能发挥最大作用。

(4) Windows Server 2008 防间谍配置：本节介绍了两款防间谍软件，通过这两款软件或类似功能的软件，管理员可以保护系统不被间谍软件侵袭，保护隐私信息不被泄露。

14.6　思考与练习

【思考题】

1. 操作系统漏洞带来的危害是否可以避免？为什么？
2. Windows Server 2008 中的高级防火墙有什么特点？
3. Windows Server 2008 中的数据执行保护功能和防病毒软件有何异同之处？
4. 病毒和间谍软件有何区别？

【练习题】

1. 如何实现 Windows 系统的手动更新？
2. 怎么实现服务器的自动升级更新？
3. 如何在高级防火墙中关闭一个指定端口？
4. 防病毒软件有何不足之处？

第15章　综合应用案例

【本章导读】

本章将构建一个功能较齐全的网络应用系统，以巩固前面介绍的主要 Windows Server 2008 技术。

15.1　网络结构设计与联接

15.1.1　网络拓扑结构设计

如图 15-1 所示的是一个中小型的计算机网络，能提供常用的所有功能，通过扩充拓扑结构，可演变为更大、更小的网络规模。

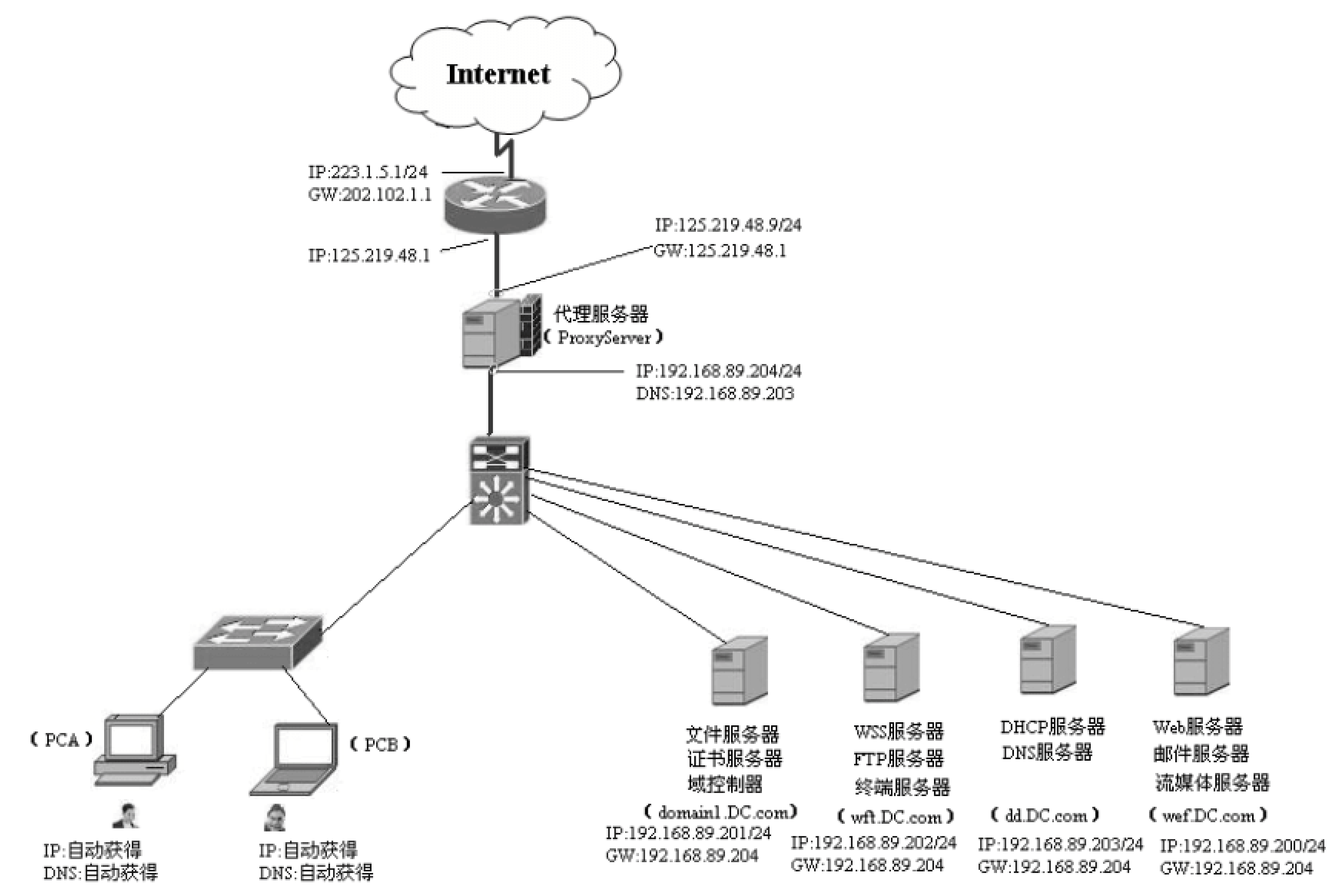


图 15-1　综合应用案例采用的网络拓扑

路由器以上为代表外网的 Internet，以下为内部网络，内部网络通过路由器接入外网。在内部网络中，有若干台客户端主机和专用的服务器主机。客户端主机通过二层交换机、三层交换机、代理服务器和路由器访问外网，不允许外网访问内网中的任何主机。

15.1.2　网络连接

首先进行硬件连接，然后配置网络设备，以实现网络连接。

1. 网络连接

外网、代理服务器、三层交换机之间可采用光纤连接，也可用五类双绞线连接；二层交换机、三层交换机及其他设备之间采用五类双绞线连接。三层交换机也可用二层交换机代替。

两台 PC 客户机也可以用一台代替。若服务器主机的性能足够高，也可以将服务器集中到更少的主机上实现。

2. 配置网络设备

路由器、客户端主机、服务器主机的 IP 地址等网络参数进行配置和测试，确保它们之间的链路能够互联互通。

15.2　主机系统配置

15.2.1　客户端主机的系统配置

客户端主机可安装任何版本的网络操作系统。推荐采用不同于 Windows Server 2008 的操作系统，如 Linux、Windows XP 等。

15.2.2　服务器主机的系统配置

代理服务器安装 Windows Server 2008 操作系统，不加入域；各服务器均安装 Windows Server 2008 操作系统，均加入域。具体配置如下。

1. 域控制器的配置

(1) 主机 NetBIOS 名：domain1；

(2) 域名：DC.com；

(3) 主机域名：domain1.DC.com；

(4) 活动目录的安装、域控制器的配置，方法详见第 1 章、第 5 章；

(5) 域控制器的测试：设置客户端主机 PCA 的 IP 地址如下。

① IP：192.168.89.100；

② 子网掩码：255.255.255.0；

③ 网关：无；

④ DNS：192.168.89.203；

(6) 参考第 5 章，将客户端主机 PCA 加入域 DC.com，若成功地登录域控制器，说明域控制器配置成功。

2. 证书服务器的配置

(1) 主机 NetBIOS 名：domain1；

(2) 域名：DC.com；

(3) 主机域名：domain1.DC.com；

(4) 证书服务器的安装、配置(方法详见第 6 章)；

(5) 证书服务器的测试：设置客户端主机 PCB 的 IP 地址如下。

① IP：192.168.89.101；

② 子网掩码：255.255.255.0；

③ 网关：无；

④ DNS：192.168.89.203；

(6) 参考第 6 章，PCA 和 PCB 分别向证书服务器申请证书、安装证书，并通过验证证书互相访问，若访问成功，说明证书服务器配置基本成功；待到配置成功 Web 服务器后，Web 服务器向证书服务器申请证书、安装证书，PCA 能够通过 HTTPS 协议访问 Web 服务器，说明证书服务器配置完全成功。

3. 文件服务器的配置

(1) 主机 NetBIOS 名：domain1；

(2) 域名：DC.com；

(3) 主机域名：domain1.DC.com；

(4) 文件服务器的安装、配置(方法详见第 2 章)；

(5) 文件服务器的测试：参考第 2 章，将文件服务器上不同文件夹的不同访问权限授权给两名客户端主机用户，两名用户录入自己的域帐号登录文件服务器并在授权范围内访问文件夹内资源，然后再试图越权访问资源，若能且只能在授权范围内访问资源，说明文件服务器配置成功。

4. WSS 服务器的配置

(1) 主机 NetBIOS 名：wft；

(2) 域名：DC.com；

(3) 主机域名：wft.DC.com；

(4) WSS 服务器的安装、配置(方法详见第 1 章、第 3 章)；

(5) WSS 服务器的测试：参考第 3 章，两名客户端主机用户访问 WSS 站点共享的资源，若能在授权范围内访问资源，说明 WSS 服务器配置成功。

5. FTP 服务器的配置

(1) 主机 NetBIOS 名：wft；

(2) 域名：DC.com；

(3) 主机域名：wft.DC.com；

(4) FTP 服务器的安装、配置(方法详见第 9 章)；

(5) FTP 服务器的测试：参考第 9 章，两名客户端主机用户访问 FTP 服务器的资源，若能在授权范围内访问资源，说明 FTP 服务器配置成功。

6. 终端服务器的配置

(1) 主机 NetBIOS 名：wft；

(2) 域名：DC.com；

(3) 主机域名：wft.DC.com；

(4) 终端服务器的安装、配置(方法详见第 12 章)；

(5) 终端服务器的测试：参考第 12 章，一名客户端主机用户访问终端服务器的资源，若能在授权范围内访问资源，说明终端服务器配置成功。

7. Web 服务器的配置

(1) 主机 NetBIOS 名：wef；

(2) 域名：DC.com；

(3) 主机域名：wef.DC.com；

(4) Web 服务器的安装、配置(方法详见第 1 章、第 8 章)；

(5) Web 服务器的测试：参考第 8 章，一名客户端主机用户通过 IE 浏览器和“http://192.168.89.200”访问 Web 服务器，若能访问 Web 服务器上存放的网页，说明 Web 服务器配置成功。

8. DNS 服务器的配置

(1) 主机 NetBIOS 名：dd；

(2) 域名：DC.com；

(3) 主机域名：dd.DC.com；

(4) DNS 服务器的安装、配置(方法详见第 1 章、第 4 章)；

(5) DNS 服务器的测试：参考第 8 章，将“wef.DC.com”配置到主机头，参考第 4 章，对该主机头进行正向和逆向解析，一名客户端主机用户通过 IE 浏览器和“http://192.168.89.200”访问 Web 服务器，若能访问 Web 服务器上存放的网页，并且在 DOS 系统下执行说明 Web 命令“ping 192.168.89.200”能看到主机头“wef.DC.com”，说明 DNS 服务器配置成功。

9. DHCP 服务器的配置

(1) 主机 NetBIOS 名：dd；

(2) 域名：DC.com；

(3) 主机域名：dd.DC.com；

(4) 地址池：192.168.89.1-192.168.89.199；

(5) 自动分配：其他服务器的 IP 地址；

(6) DHCP 服务器的安装、配置(方法详见第 7 章)；

(7) DHCP 服务器的测试：将客户端主机 PCA 和 PCB 的 IP 地址和 DNS 地址恢复成自动获得，参考第 7 章，若主机 PCA 能访问以上任一服务器，说明 DHCP 服务器配置成功。

10. 邮件服务器的配置

(1) 主机 NetBIOS 名：wef；

(2) 域名：DC.com；

(3) 主机域名：wef.DC.com；

(4) 邮件服务器的安装、配置(方法详见第 10 章)；

(5) 邮件服务器的测试：参考第 10 章，若主机 PCA 能访问以上邮件服务器，说明邮件服务器配置成功。

11. 流媒体服务器的配置

(1) 主机 NetBIOS 名：wef；

(2) 域名：DC.com；

(3) 主机域名：wef.DC.com；

(4) 流媒体服务器的安装、配置(方法详见第 11 章)；

(5) 流媒体服务器的测试：参考第 11 章，若主机 PCA 能访问流媒体服务器存放的授权资源，说明流媒体服务器配置成功。

12. 代理服务器的配置

(1) 主机 NetBIOS 名：ProxyServer；

(2) 域名：DC.com；

(3) 主机域名：wef.DC.com；

(4) 代理服务器的安装、配置、防间谍和防病毒配置(方法详见第 1 章、第 13 章、第 14 章)；

(5) 代理服务器的测试：参考第 13 章、第 14 章，若主机 PCA 能访问外网的资源，说明代理服务器配置成功。

15.3　本章小结

本章主要介绍了多种主流 Windows Server 2008 服务器的安装、配置和测试的方法，这对于巩固读者对 Windows Server 2008 知识的理解和操作技能的运用起到明显的作用。

15.4　思考与练习

【思考题】

1. 网络连接分为几步完成？
2. 测试证书服务器为什么分两步？

【练习题】

如何测试 DNS 服务器？(参考 15.2.3 节.8)

参 考 文 献

[1] 戴有炜. Windows Server 2008 网络专业指南. 北京：科学出版社，2009.

[2] Jeffrey R. Shapiro. Windows Server 2008 Bible. Italy:Hoepli，2009.

[3] 李书满，杜卫国. Windows Server 2008 服务器搭建与管理. 北京：清华大学出版社，2010.

[4] IT 同路人. 完全掌握 Windows Server 2008 系统管理、活动目录、服务器架设. 北京：人民邮电出版社，2009.

[5] 尚冬娟. 服务器架设技术基础与实践教程. 北京：电子工业出版社，2010.

[6] 邹县芳，胡昆鹏. 基于 WINDOWS 平台中的服务器配置与管理. 北京：中国铁道出版社，2008.

[7] 刘晓辉，陈洪彬. Windows Server 2008 服务器配置及管理实战详解. 北京：化学工业出版社，2010.

[8] 刘晓辉，李书满. WINDOWS SERVER 2008 服务器架设与配置实战指南. 北京：清华大学出版社，2010.

[9] 吕强，富万利. Windows Server 2008 服务器完全技术宝典. 北京：中国铁道出版社，2010.

[10] 刘晓辉，李利军. Windows Server 2008 安全内幕. 北京：清华大学出版社，2009.